Supplemento ordinario alla "Gazzetta Ufficiale" n. 167 del 21 luglio 2003 - Serie generale

Spediz. abb. post. 45% - art. 2, comma 20/b
Legge 23-12-1996, n. 662 - Filiale di Roma

DELLA REPUBBLICA ITALIANA

PARTE PRIMA **Roma - Lunedì, 21 luglio 2003** SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DIREZIONE E REDAZIONE PRESSO IL MINISTERO DELLA GIUSTIZIA - UFFICIO PUBBLICAZIONE LEGGI E DECRETI - VIA ARENULA 70 - 00100 ROMA
AMMINISTRAZIONE PRESSO L'ISTITUTO POLIGRAFICO E ZECCA DELLO STATO - LIBRERIA DELLO STATO - PIAZZA G. VERDI 10 - 00100 ROMA - CENTRALINO 06 85081

N. 114

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI
11 aprile 2003.

Norme di sicurezza per la tutela delle informazioni UE classificate, di attuazione della Decisione della Commissione delle Comunità europee del 29 novembre 2001.

SOMMARIO

DECRETI PRESIDENZIALI

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 11 aprile 2003.

Norme di sicurezza per la tutela delle informazioni UE classificate, di attuazione della Decisione della Commissione delle Comunità europee del 29 novembre 2001.

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Vista la legge 24 ottobre 1977, n. 801, recante «Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato», in particolare articoli 1, secondo comma, e 12;

Vista la Decisione della Commissione delle Comunità europee n. 2001/844/CE, CECA, Euratom della Commissione europea del 29 novembre 2001, che modifica il regolamento interno della medesima Commissione, pubblicata nella Gazzetta Ufficiale delle Comunità europee n. L 317 del 3 dicembre 2001, in particolare l'articolo 2, paragrafo 2, dell'Allegato, secondo cui gli Stati membri sono autorizzati a ricevere informazioni classificate UE a condizione che essi garantiscano che, nel trattare tali informazioni, siano rispettate nelle loro sedi di servizio disposizioni strettamente equivalenti a quelle menzionate nell'articolo 1 della medesima Decisione, in particolare da parte:

a) dei membri della Rappresentanza permanente d'Italia presso l'Unione europea, nonché dei membri di delegazioni nazionali che partecipano alle riunioni della Commissione o dei suoi organi o che prendono parte ad altre attività della Commissione;

b) di altri membri delle amministrazioni nazionali che trattano informazioni classificate UE, i quali prestino servizio nel territorio dello Stato o all'estero.

Visto il decreto del Presidente del Consiglio dei Ministri del 21 settembre 1999;

Viste le direttive del Presidente del Consiglio dei Ministri/Autorità nazionale per la sicurezza:

PCM-ANS l/R — Norme unificate per la tutela del segreto di Stato - Volume I - Sistema di Sicurezza - Edizione 1987 e successive modificazioni e integrazioni;

PCM-ANS 1/R — Norme unificate per la tutela del segreto di Stato - Volume II - Sicurezza delle comunicazioni ed organizzazioni e procedure del servizio cifra - Edizione 1994;

PCM-ANS 1/R — Norme unificate per la tutela del segreto di Stato - Volume III - Sicurezza Industriale - Edizione 1993;

PCM-ANS 1/R/A — Norme unificate per la tutela del segreto di Stato - Volume I - Direttiva per la protezione delle informazioni coperte dal segreto di Stato trattate in sistemi di elaborazione automatica e/o elettronica dei dati (EAD) - Edizione 1993;

PCM-ANS COMSEC 256 (B) — Norme relative all'installazione di apparati elettrici/elettronici che elaborano informazioni classificate - Edizione 1998;

Visto il decreto del Presidente del Consiglio dei Ministri 11 aprile 2002, n. 130, recante «Norme di sicurezza per la tutela delle informazioni UE classificate di attuazione della Decisione del Consiglio dell'Unione europea del 19 marzo 2001», in particolare l'Allegato 2 al medesimo;

Ritenuta l'esigenza di dare, per gli aspetti interni, piena attuazione alla predetta Decisione della Commissione dell'Unione europea 2001/844/CE, CECA, Euratom;

ADOTTA

il seguente decreto:

Art. 1.

1. Per gli aspetti di rilevanza interna, piena e completa attuazione è data alla Decisione 2001/844/CE, CECA, Euratom della Commissione delle Comunità europee del 29 novembre 2001, che modifica il regolamento interno della Commissione, pubblicata nella Gazzetta Ufficiale delle Comunità europee n. L 317 del 3 dicembre 2001, di cui all'Allegato 1.

2. Si applicano, ai fini dell'aggiornamento dell'organizzazione nazionale per la sicurezza per la tutela delle informazioni classificate, le disposizioni di cui all'Allegato 2 al decreto del Presidente del Consiglio dei Ministri 11 aprile 2002, n. 130.

3. L'Autorità nazionale per la sicurezza prescrive le altre disposizioni di dettaglio per l'integrale attuazione delle norme di sicurezza contenute nella predetta Decisione, nell'ambito nazionale e nel rispetto della disciplina di protezione dei dati personali, eventualmente applicabile.

4. Il presente decreto è pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 11 aprile 2003

Il Presidente: BERLUSCONI

ALLEGATO 1

II

(Atti per i quali la pubblicazione non è una condizione di applicabilità)

COMMISSIONE

DECISIONE DELLA COMMISSIONE
del 29 novembre 2001
che modifica il regolamento interno della Commissione

[notificata con il numero C(2001) 3031]

(2001/844/CE, CECA, Euratom)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 218, paragrafo 2,

visto il trattato che istituisce la Comunità europea del carbone e dell'acciaio, in particolare l'articolo 16,

visto il trattato che istituisce la Comunità europea dell'energia atomica, in particolare l'articolo 131,

visto il trattato sull'Unione europea, in particolare l'articolo 28, paragrafo 1, e l'articolo 41, paragrafo 1,

DECIDE:

Articolo 1

Le disposizioni della Commissione in materia di sicurezza, il cui testo è allegato alla presente decisione, sono aggiunte in allegato al regolamento interno della Commissione.

Articolo 2

La presente decisione entra in vigore il giorno della pubblicazione nella *Gazzetta ufficiale delle Comunità europee*.

Essa si applica a decorrere dal 1° dicembre 2001.

Fatto a Bruxelles, il 29 novembre 2001.

Per la Commissione
Il Presidente
Romano PRODI

DISPOSIZIONI DELLA COMMISSIONE

Considerando quanto segue:

(1) Per sviluppare le attività della Commissione in settori che richiedono un certo grado di riservatezza, occorre porre in essere un sistema di sicurezza globale riguardante la Commissione, le altre istituzioni, organi, uffici e agenzie istituiti in base al trattato CE o al trattato sull'Unione europea, gli Stati membri, nonché qualunque altro destinatario di informazioni classificate UE, di seguito denominate «informazioni classificate UE».

(2) Per salvaguardare l'efficienza del sistema di sicurezza così istituito, la Commissione consentirà l'accesso alle informazioni classificate UE soltanto a quegli organismi esterni che dimostrino di aver preso tutte le misure necessarie per conformarsi a disposizioni strettamente equivalenti alle presenti disposizioni.

(3) Le presenti disposizioni lasciano impregiudicati il regolamento n. 3, del 31 luglio 1958, recante attuazione dell'articolo 24 del trattato che istituisce la Comunità europea dell'energia atomica (¹); il regolamento (CE) n. 1588/90 del Consiglio, dell'11 giugno 1990, relativo alla trasmissione all'Istituto statistico delle Comunità europee di dati statistici protetti dal segreto (²), nonché la decisione C (95) 1510 def. della Commissione, del 23 novembre 1995, sulla protezione dei sistemi informatici.

(4) La Commissione fonda il proprio sistema di sicurezza sui principi enunciati nella decisione 2001/264/CE del Consiglio, del 19 marzo 2001, che adotta le norme di sicurezza del Consiglio (³), allo scopo di assicurare il buon funzionamento del processo decisionale dell'Unione.

(5) La Commissione sottolinea l'importanza di associare, ove opportuno, le altre istituzioni dell'Unione europea alle regole e alle norme di riservatezza necessarie per tutelare gli interessi dell'Unione e degli Stati membri.

(6) La Commissione riconosce la necessità di creare un proprio concetto di sicurezza, prendendo in considerazione tutti gli elementi della sicurezza ed il carattere peculiare della Commissione in quanto istituzione.

(7) Le presenti disposizioni lasciano impregiudicati l'articolo 255 del trattato e il regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (⁴).

Articolo 1

Le disposizioni della Commissione in materia di sicurezza sono riportate nell'allegato.

Articolo 2

1. Il membro della Commissione preposto alla sicurezza prende le misure necessarie per garantire che, nel trattare informazioni classificate UE, i funzionari e gli altri agenti della Commissione, il personale distaccato presso la Commissione, il personale impiegato in tutte le sedi della Commissione, compresi gli uffici di rappresentanza nell'Unione e le delegazioni nei paesi terzi, nonché i contraenti esterni della Commissione rispettino le disposizioni di cui all'articolo 1.

2. Gli Stati membri, nonché le altre istituzioni, organi, uffici ed agenzie istituiti dai trattati o in base ad essi sono autorizzati a ricevere informazioni classificate UE a condizione che essi garantiscano che, nel trattare tali informazioni, siano rispettate nelle loro sedi di servizio disposizioni strettamente equivalenti a quelle menzionate all'articolo 1, in particolare da parte:

a) dei membri delle rappresentanze permanenti degli Stati membri presso l'Unione europea, nonché dei membri di delegazioni nazionali che partecipano alle riunioni della Commissione o dei suoi organi o che prendono parte ad altre attività della Commissione;

b) di altri membri delle amministrazioni nazionali degli Stati membri che trattano informazioni classificate UE, i quali prestino servizio nel territorio degli Stati membri o all'estero;

c) di contraenti esterni e di personale distaccato che trattano informazioni classificate UE.

(¹) GU n. 17 del 6.10.1958, pag. 406/58.
(²) GU L 151 del 15.6.1990, pag. 1.
(³) GU L 101 dell'11.4.2001, pag. 1.
(⁴) GU L 145 del 31.5.2001, pag. 43.

Articolo 3

Gli Stati terzi, le organizzazioni internazionali ed altri organismi sono autorizzati a ricevere informazioni classificate UE a condizione che essi garantiscano che, nel trattare tali informazioni, siano rispettate disposizioni strettamente equivalenti a quelle menzionate all'articolo 1.

Articolo 4

Conformemente ai principi fondamentali e alle norme minime di sicurezza contenuti nella parte I dell'allegato, il membro della Commissione preposto alla sicurezza può adottare misure ai sensi della parte II dell'allegato.

Articolo 5

A decorrere dalla data della loro applicazione, le presenti disposizioni sostituiscono:

a) la decisione C (94) 3282 della Commissione, del 30 novembre 1994, relativa alle misure di sicurezza applicabili alle informazioni classificate prodotte o trasmesse nel quadro delle attività dell'Unione europea;

b) la decisione C (1999) 423 della Commissione, del 25 febbraio 1999, relativa alle modalità secondo cui i funzionari e gli agenti della Commissione europea possono essere autorizzati ad accedere a informazioni classificate in possesso della Commissione.

Articolo 6

A decorrere dalla data di applicazione delle presenti disposizioni, tutte le informazioni classificate in possesso della Commissione fino a tale data, eccetto le informazioni classificate Euratom,

a) se sono state create dalla Commissione, si considerano riclassificate per difetto «RISERVATO UE», a meno che l'autore decida di conferire loro un'altra classificazione entro il 31 gennaio 2002, nel qual caso l'autore ne informa tutti i destinatari del documento in questione;

b) se sono state create da fonti esterne alla Commissione, conservano la classificazione originaria e sono quindi trattate come informazioni classificate UE di grado equivalente, a meno che l'autore acconsenta a declassificarle o declassarle.

DISPOSIZIONI IN MATERIA DI SICUREZZA

Indice

PARTE I: PRINCIPI FONDAMENTALI E NORME MINIME DI SICUREZZA

1. INTRODUZIONE

Con queste disposizioni si stabiliscono i principi fondamentali e le norme minime di sicurezza che devono essere debitamente rispettate dalla Commissione in tutte le sue sedi di servizio e da tutti i destinatari di informazioni classificate UE, perché sia salvaguardata la sicurezza e ognuno abbia la garanzia che è in vigore un regime comune di protezione.

2. PRINCIPI GENERALI

La politica di sicurezza della Commissione forma parte integrante della sua politica generale di gestione interna e si basa pertanto sugli stessi principi informatori di quest'ultima.

Tra questi principi si annoverano la legalità, la trasparenza, la responsabilità (o dovere di rendere conto delle proprie azioni) e la sussidiarietà (o proporzionalità).

Per legalità si intende la stretta adesione al quadro giuridico nell'espletamento delle funzioni legate alla sicurezza e la rigorosa ottemperanza alle prescrizioni legali. Questo concetto implica altresì che le responsabilità nel campo della sicurezza si fondino su adeguate disposizioni normative. Tra queste, trovano piena applicazione le disposizioni dello statuto del personale, segnatamente l'articolo 17 sull'obbligo di discrezione imposto al personale riguardo alle informazioni della Commissione e il titolo VI sulle misure disciplinari. Un'altra implicazione, infine, è che le violazioni della sicurezza nell'ambito di responsabilità della Commissione devono essere affrontate in maniera coerente con la politica della Commissione in materia disciplinare e con la sua politica di cooperazione con gli Stati membri in campo penale e giudiziario.

Per trasparenza si intende chiarezza in tutte le norme e disposizioni sulla sicurezza, equilibrio nella ripartizione delle competenze tra i vari servizi e settori (sicurezza materiale, protezione delle informazioni, ecc.) e un'azione sistematica e strutturata di coscientizzazione alla tematica della sicurezza. Oltre a ciò, questo termine presuppone l'esistenza di chiari orientamenti scritti per l'attuazione delle misure di sicurezza.

Per responsabilità si intende innanzi tutto una chiara definizione delle competenze in materia di sicurezza, da cui discende la necessità di una regolare verifica del corretto esercizio di tali competenze.

Sussidiarietà, o proporzionalità, significa che la sicurezza dev'essere organizzata al livello gerarchico più basso, il più possibile in connessione con le direzioni generali e con i servizi della Commissione. Inoltre, gli interventi nel campo della sicurezza devono essere limitati allo stretto indispensabile e, infine, le misure di sicurezza devono essere proporzionate agli interessi da tutelare e alle minacce, reali o potenziali, contro tali interessi, i quali vanno comunque difesi con il minor danno possibile.

3. FONDAMENTI DELLA SICUREZZA

Un'efficace sicurezza si fonda sui seguenti elementi:

a) all'interno di ciascuno Stato membro, un'organizzazione della sicurezza nazionale competente per:

   1) la raccolta e la registrazione di informazioni in materia di spionaggio, sabotaggio, terrorismo e altre attività sovversive;

   2) l'informazione e la consulenza al proprio governo e, tramite quest'ultimo, alla Commissione, circa il carattere delle minacce che incombono sulla sicurezza e i relativi mezzi di protezione;

b) all'interno di ciascuno Stato membro e nell'ambito della Commissione, un'autorità tecnica INFOSEC incaricata di collaborare con l'autorità di sicurezza competente per fornire informazioni e consulenza circa le minacce tecniche alla sicurezza e i relativi mezzi di protezione;

c) una regolare collaborazione tra amministrazioni pubbliche e i servizi competenti delle istituzioni europee per stabilire e raccomandare opportunamente:

   1) quali persone, informazioni e risorse occorre proteggere;

   2) norme comuni di protezione;

d) una stretta collaborazione tra l'Ufficio di sicurezza della Commissione e i servizi di sicurezza delle altre istituzioni europee, nonché con l'Ufficio di sicurezza della NATO (NOS).

4. PRINCIPI DI SICUREZZA DELLE INFORMAZIONI

4.1. Obiettivi

La sicurezza delle informazioni persegue principalmente i seguenti obiettivi:

a) proteggere le informazioni classificate UE dallo spionaggio, da manomissioni o dalla diffusione non autorizzata;

b) proteggere le informazioni UE impiegate in sistemi e reti di comunicazione e d'informazione da minacce contro la loro riservatezza, integrità e disponibilità;

c) proteggere le installazioni in cui si trovano le informazioni UE dal sabotaggio e dal danneggiamento intenzionale premeditato;

d) qualora sia impossibile evitarlo, valutare il danno arrecato, limitarne le conseguenze e adottare le misure necessarie per ripararlo.

4.2. Definizioni

Ai fini delle presenti disposizioni, si intende per:

a) «informazioni classificate UE» (ICUE): le informazioni e i materiali la cui divulgazione non autorizzata potrebbe recare in varia misura pregiudizio agli interessi dell'UE o a uno o più Stati membri, sia che le informazioni suddette provengano dall'interno dell'UE ovvero dagli Stati membri, da Stati terzi o da organizzazioni internazionali;

b) «documento»: qualsiasi lettera, nota, verbale, relazione, promemoria, segnale/messaggio, schizzo, fotografia, diapositiva, pellicola, mappa, diagramma, piano, taccuino, stampo, carta carbone, nastro dattilografico o di stampante, nastro magnetico, cassetta, dischetto di computer, CD ROM o altro mezzo materiale sul quale possono essere state registrate informazioni;

c) «materiale»: qualsiasi «documento» secondo la definizione di cui alla lettera b) e altresì qualsiasi elemento di attrezzatura, sia sotto forma di prodotto finito, sia in corso di lavorazione;

d) «necessità di sapere»: la necessità di un singolo dipendente di accedere ad informazioni classificate UE per poter espletare una funzione o eseguire una mansione;

e) «autorizzazione»: una decisione del presidente della Commissione con cui si concede l'accesso individuale ad informazioni classificate UE fino ad un determinato grado, sulla base dell'esito positivo di un'indagine di sicurezza svolta da un'autorità nazionale competente a norma del diritto nazionale;

f) «classificazione»: il conferimento di un idoneo livello di sicurezza ad informazioni la cui divulgazione non autorizzata potrebbe recare in certa misura pregiudizio agli interessi della Commissione o degli Stati membri;

g) «declassamento»: una riduzione del grado di classificazione;

h) «declassificazione»: la soppressione di qualsiasi menzione di classificazione;

i) «originatore»: l'autore debitamente autorizzato di un documento classificato. All'interno della Commissione, i capi dei servizi possono autorizzare i loro subordinati ad «originare» ICUE;

j) «servizi della Commissione»: le direzioni generali e i vari servizi della Commissione, compresi i gabinetti, in tutte le sedi di servizio, inclusi il Centro Comune di Ricerca, gli uffici di rappresentanza nell'Unione e le delegazioni nei paesi terzi.

4.3. Classificazione

a) Per quanto riguarda la riservatezza, la selezione delle informazioni e dei materiali da proteggere e la valutazione del grado di protezione necessaria richiedono diligenza ed esperienza. È particolarmente importante che il grado di protezione corrisponda al grado di sicurezza richiesto dalla singola informazione e dal singolo materiale da proteggere. Perché non vi siano ostacoli al flusso delle informazioni, occorre prendere provvedimenti per evitare sia la sovra-classificazione che la sottoclassificazione.

b) Il sistema di classificazione è lo strumento per tradurre in pratica questi principi; un sistema di classificazione analogo dovrebbe essere adottato nella pianificazione e nell'organizzazione della lotta contro lo spionaggio, il sabotaggio, il terrorismo e altre minacce, in modo da garantire la massima protezione ai principali edifici in cui sono collocate informazioni classificate e i punti più sensibili all'interno di questi.

c) La responsabilità della classificazione delle informazioni spetta unicamente all'originatore.

d) Il grado di classificazione dipende unicamente dal contenuto delle informazioni stesse.

e) Se più elementi d'informazione sono uniti congiuntamente, il grado di classificazione da conferire all'insieme sarà almeno equivalente a quello dell'elemento con grado più elevato. Ad una raccolta di informazioni può essere tuttavia conferito un grado di classificazione più elevato di quello dei suoi elementi costitutivi.

f) Le classificazioni devono essere assegnate soltanto nella misura e per la durata in cui sia necessario.

4.4. Finalità delle misure di sicurezza

Le misure di sicurezza:

a) riguardano tutte le persone che hanno accesso alle informazioni classificate, ai relativi supporti, agli edifici che contengono tali informazioni e a importanti installazioni;

b) sono destinate a individuare le persone che, per la loro situazione, potrebbero mettere in pericolo la sicurezza di informazioni classificate o di importanti installazioni che contengono informazioni classificate e a provvedere alla loro esclusione o allontanamento;

c) impediscono alle persone non autorizzate di accedere alle informazioni classificate o alle installazioni che le contengono;

d) garantiscono che le informazioni classificate siano diffuse soltanto in base al principio della necessità di sapere, che è fondamentale per tutti gli aspetti della sicurezza;

e) assicurano l'integrità (ossia la prevenzione della corruzione, dell'alterazione o della cancellazione non autorizzate) e la disponibilità (ossia che l'accesso non sia negato a coloro che devono e sono autorizzati ad averlo) di tutte le informazioni, siano esse classificate o non, e soprattutto delle informazioni immagazzinate, elaborate o trasmesse sotto forma elettromagnetica.

5. ORGANIZZAZIONE DELLA SICUREZZA

5.1. Norme comuni minime

La Commissione garantisce che tutti i destinatari di ICUE, all'interno dell'istituzione e nei servizi soggetti alla sua competenza, compresi i contraenti, osservino norme minime comuni di sicurezza affinché le informazioni classificate UE possano essere trasmesse con la certezza che saranno trattate con la stessa diligenza. Dette norme minime includono criteri per il rilascio del nulla osta di sicurezza al personale e procedure per la protezione delle informazioni classificate UE.

La Commissione autorizza l'accesso alle ICUE ad organismi esterni solo a condizione che essi garantiscano che, nel trattare le ICUE, siano rispettate disposizioni strettamente equivalenti alle suddette norme minime.

5.2. Organizzazione

All'interno della Commissione, la sicurezza è organizzata a due livelli:

a) a livello della Commissione nel suo insieme, esiste un ufficio di sicurezza della Commissione, di cui fanno parte un'autorità di accreditamento in materia di sicurezza (SAA) — che funge anche da autorità Crypto (CrA) e da autorità TEMPEST — ed un'autorità INFOSEC (IA), affiancato da uno o più uffici centrali di registrazione per le ICUE, ciascuno con uno o più funzionari di controllo (RCO);

b) a livello dei singoli servizi della Commissione, la competenza in materia di sicurezza è ripartita tra uno o più responsabili della sicurezza a livello locale (LSO), uno o più responsabili della sicurezza informatica a livello centrale (CISO), responsabili della sicurezza informatica a livello locale (LISO) e uffici locali di registrazione per le ICUE con uno o più funzionari di controllo;

c) gli organi di sicurezza centrali impartiscono istruzioni operative agli organi di sicurezza locali.

6. SICUREZZA DEL PERSONALE

6.1. Nulla osta di sicurezza del personale

Tutti coloro che devono accedere a informazioni classificate UE RISERVATISSIMO o di grado superiore devono aver debitamente ricevuto l'apposito nulla osta prima di essere autorizzate a tale accesso. Lo stesso nulla osta è richiesto alle persone che si occupano del funzionamento tecnico o della manutenzione dei sistemi di comunicazione e di informazione contenenti informazioni classificate. Questo nulla osta deve servire a determinare se detti individui:

a) sono di indefettibile lealtà;

b) dimostrano forza di carattere e discrezione tali che non vi siano dubbi sulla loro integrità nel trattamento delle informazioni classificate; oppure

c) possono essere sensibili a pressioni provenienti dall'esterno o altre.

Nell'ambito delle procedure di nulla osta, sono sottoposti ad un esame particolarmente accurato coloro che:

d) devono ottenere accesso alle informazioni UE SEGRETISSIMO;

e) occupano posizioni per le quali hanno regolare accesso a una considerevole quantità di informazioni UE SEGRETO;

f) hanno per le loro mansioni accesso speciale a sistemi di comunicazione o d'informazione protetti e perciò potrebbero avere accesso non autorizzato a grandi quantità di informazioni classificate UE o danneggiare gravemente la missione con atti di sabotaggio tecnico.

Nelle circostanze di cui alle lettere d), e) e f) si deve impiegare nella massima misura possibile la tecnica delle indagini di fondo.

Le persone che non hanno una vera e propria «necessità di sapere» e lavorano in circostanze nelle quali possono avere accesso a informazioni classificate UE (per esempio fattorini, agenti della sicurezza, personale addetto alla manutenzione o alle pulizie ecc.), devono prima di tutto ottenere un apposito nulla osta di sicurezza.

6.2. Registrazione dei nulla osta del personale

Tutti i servizi della Commissione che trattano informazioni classificate UE ovvero ospitano sistemi di comunicazione o d'informazione protetti tengono una traccia dei nulla osta concessi al personale addetto. Ciascun nulla osta deve essere verificato all'occorrenza, per accertare che sia adatto ai compiti svolti da quella persona; deve essere immediatamente riesaminato non appena nuove informazioni indichino che non è più nell'interesse della sicurezza mantenere quella persona a contatto con informazioni classificate. Il responsabile della sicurezza a livello locale presso il servizio interessato tiene una traccia dei nulla osta che rientrano nella sua sfera di competenza.

6.3. Istruzioni di sicurezza per il personale

Tutto il personale che ricopre incarichi in cui potrebbe aver accesso a informazioni classificate è dettagliatamente istruito al momento di assumere l'incarico e a intervalli regolari circa le esigenze di sicurezza e le relative procedure. Detto personale è tenuto a certificare per iscritto di aver letto e perfettamente capito le presenti norme di sicurezza.

6.4. Responsabilità dei dirigenti

I dirigenti hanno il dovere di sapere quali dei loro subordinati lavorino a contatto con informazioni classificate o abbiano accesso a sistemi di comunicazione o d'informazione protetti e di registrare e riferire qualsiasi incidente o caso di palese vulnerabilità che possa avere conseguenze sulla sicurezza.

6.5. Affidabilità del personale in fatto di sicurezza

Sono istituite procedure per garantire che, allorché si viene a conoscenza di informazioni negative riguardo a un individuo, si chiarisca se costui svolge un lavoro a contatto con informazioni classificate o ha accesso a sistemi di comunicazione o d'informazione protetti e l'ufficio di sicurezza ne sia informato. Se si stabilisce che rappresenta un pericolo per la sicurezza, detto individuo deve essere allontanato o rimosso da ogni incarico in cui potrebbe mettere a repentaglio la sicurezza.

7. SICUREZZA MATERIALE

7.1. Necessità della protezione

Il grado di sicurezza materiale da applicare per garantire la protezione delle informazioni classificate UE deve essere proporzionato alla classificazione, al volume e alle minacce che incombono sulle informazioni e sul materiale custodito. Tutti i detentori di informazioni classificate UE devono seguire pratiche uniformi per quanto riguarda la classificazione delle informazioni in loro possesso e ottemperare a norme comuni di protezione per quel che riguarda la custodia, la trasmissione e la diffusione di informazioni e di materiale soggetti a protezione.

7.2. Controlli

Prima di lasciare i luoghi in cui sono riposte informazioni classificate UE, non sottoposti a sorveglianza, le persone a cui detti luoghi sono affidati devono assicurarsi che le informazioni siano immagazzinate in modo sicuro e che tutti i dispositivi di sicurezza siano stati attivati (serrature, allarmi, ecc.). Al termine dell'orario di lavoro devono essere effettuati altri controlli indipendenti.

7.3. **Sicurezza degli edifici**

Gli edifici contenenti informazioni classificate UE o sistemi di comunicazione e d'informazione protetti devono essere tutelati contro l'accesso non autorizzato. Il tipo di protezione destinato alle informazioni classificate UE, per esempio sbarramento di finestre, serrature alle porte, guardie all'entrata, sistemi di controllo dell'accesso automatizzati, controlli di sicurezza e ispezioni, sistemi d'allarme, sistemi di individuazione delle intrusioni e cani da guardia dipendono:

a) dalla classificazione, dal volume e dall'ubicazione all'interno dell'edificio delle informazioni e dei materiali da proteggere;

b) dalla qualità dei contenitori di sicurezza per queste informazioni e materiali;

c) dalle caratteristiche dell'edificio e dalla sua ubicazione.

Anche per i sistemi di comunicazione e d'informazione il tipo di protezione prescelto deve dipendere da una stima del valore di quanto è in gioco e del danno potenziale che deriverebbe dal venir meno della sicurezza, dalle caratteristiche e dall'ubicazione dell'edificio nel quale è custodito il sistema e dalla collocazione del sistema all'interno dell'edificio.

7.4. **Piani d'emergenza**

Occorre predisporre in anticipo piani dettagliati per la protezione delle informazioni classificate durante un'emergenza locale o nazionale.

8. SICUREZZA DELLE INFORMAZIONI

La sicurezza delle informazioni (INFOSEC) riguarda l'individuazione e l'applicazione di misure di sicurezza per proteggere le informazioni classificate UE elaborate, immagazzinate o trasmesse in sistemi elettronici di comunicazione e d'informazione o altri, contro il venir meno della riservatezza, dell'integrità o della disponibilità, accidentale o intenzionale. Adeguate contromisure devono essere prese per prevenire l'accesso alle informazioni classificate UE da parte di utenti non autorizzati, per impedire che a utenti autorizzati sia opposto il rifiuto di accedere alle informazioni classificate UE e per prevenire l'alterazione ovvero la modificazione o la cancellazione non autorizzate di informazioni classificate UE.

9. MISURE CONTRO IL SABOTAGGIO ED ALTRE FORME DI DANNO INTENZIONALE PREMEDITATO

Le precauzioni materiali per la protezione di importanti installazioni in cui sono conservate informazioni classificate sono la migliore garanzia di sicurezza e di protezione contro il sabotaggio e il danno intenzionale premeditato, laddove il solo nulla osta del personale non basta. L'organismo nazionale competente è invitato a comunicare le informazioni raccolte in materia di spionaggio, sabotaggio, terrorismo e altre attività sovversive.

10. COMUNICAZIONE DI INFORMAZIONI CLASSIFICATE A STATI TERZI OD ORGANIZZAZIONI INTERNAZIONALI

Spetta alla Commissione decidere collegialmente se comunicare a uno Stato terzo o a un'organizzazione internazionale informazioni classificate UE. Se l'originatore delle informazioni che si vogliono comunicare non è la Commissione, quest'ultima deve anzitutto ottenere il consenso dell'originatore. Se è impossibile stabilire l'originatore, la Commissione ne assume la responsabilità.

Le informazioni classificate che la Commissione riceve da Stati terzi, da organizzazioni internazionali o da altri terzi devono essere oggetto di protezione proporzionata alla loro classificazione ed equivalente alle norme stabilite dalle presenti disposizioni per le informazioni classificate UE o alle norme più severe richieste dai terzi che comunicano l'informazione. Possono essere predisposti controlli reciproci.

I principi di cui sopra devono essere applicati in conformità delle disposizioni dettagliate della parte II, sezione 26, e delle appendici 3, 4 e 5.

PARTE II: L'ORGANIZZAZIONE DELLA SICUREZZA NELLA COMMISSIONE

11. IL MEMBRO DELLA COMMISSIONE COMPETENTE IN MATERIA DI SICUREZZA

Il membro della Commissione competente in materia di sicurezza:

a) attua la politica di sicurezza della Commissione;

b) prende in esame i problemi di sicurezza sottopostigli dalla Commissione o dai suoi organi competenti;

c) esamina le questioni che comportano cambiamenti nella politica di sicurezza della Commissione, in stretto legame con le autorità di sicurezza nazionali (o altre) degli Stati membri (in seguito denominate «NSA»).

In particolare, il membro della Commissione competente in materia di sicurezza ha tra le sue attribuzioni:

a) il coordinamento di tutte le questioni di sicurezza connesse alle attività della Commissione;

b) inviare alle autorità designate dagli Stati membri le richieste affinché le NSA predispongano i nulla osta di sicurezza per il personale impiegato alla Commissione in conformità della sezione 20;

c) ordinare indagini su qualsiasi fuga di informazioni classificate UE, che a prima vista sembri avere avuto luogo nell'ambito della Commissione;

d) chiedere alle autorità di sicurezza interessate di avviare indagini in caso di fuga di informazioni classificate UE che sembri aver avuto luogo al di fuori della Commissione e coordinare le inchieste quando sono coinvolte più autorità di sicurezza;

e) l'ispezione periodica dei dispositivi di sicurezza per la protezione delle informazioni classificate UE;

f) mantenere uno stretto legame con tutte le autorità di sicurezza interessate ai fini di un coordinamento globale della sicurezza;

g) riesaminare costantemente la politica e le procedure di sicurezza della Commissione e, se necessario, formulare le opportune raccomandazioni. A questo riguardo, il membro della Commissione competente in materia di sicurezza presenta alla Commissione il piano di ispezione annuale elaborato dall'ufficio di sicurezza della Commissione.

12. IL GRUPPO CONSULTIVO PER LA POLITICA DI SICUREZZA

È istituito un gruppo consultivo della Commissione per la politica di sicurezza. Esso è presieduto dal membro della Commissione competente in materia di sicurezza o da chi ne fa le veci ed è composto da rappresentanti delle NSA degli Stati membri. Possono essere invitati a parteciparvi anche rappresentanti di altre istituzioni europee, come pure rappresentanti degli organismi decentrati UE quando vi si discutono questioni che li riguardano.

Il gruppo consultivo della Commissione per la politica di sicurezza si riunisce a richiesta del presidente o di uno dei suoi membri. Esso ha il compito di esaminare e valutare tutte le questioni relative alla sicurezza e, se del caso, di presentare raccomandazioni alla Commissione.

13. IL COMITATO DI SICUREZZA DELLA COMMISSIONE

È istituito un comitato di sicurezza, presieduto dal Segretario generale e composto dai direttori generali del servizio giuridico, dell'amministrazione e del personale, delle relazioni esterne, della giustizia e affari interni e del centro comune di ricerca, nonché dai capi del servizio di audit interno e dell'ufficio di sicurezza della Commissione. Possono essere invitati a parteciparvi anche altri funzionari della Commissione. Esso ha il compito di valutare le misure di sicurezza vigenti all'interno della Commissione e di rivolgere raccomandazioni in materia al membro della Commissione competente per la sicurezza.

14. L'UFFICIO DI SICUREZZA DELLA COMMISSIONE

Per adempiere le responsabilità di cui alla sezione 11, il membro della Commissione competente per la sicurezza dispone dell'ufficio di sicurezza della Commissione per il coordinamento, la supervisione e l'applicazione delle misure di sicurezza.

Il capo dell'ufficio di sicurezza della Commissione è il consigliere principale del membro della Commissione competente in materia di sicurezza circa le questioni di sicurezza e funge da segretario del gruppo consultivo per la politica di sicurezza. Dirige l'aggiornamento della normativa in materia di sicurezza e coordina le misure di sicurezza con le autorità competenti degli Stati membri e, se del caso, con le organizzazioni internazionali che hanno concluso con la Commissione accordi in materia di sicurezza. A questo scopo agisce come ufficiale di collegamento.

Il capo dell'ufficio di sicurezza della Commissione è responsabile dell'accreditamento dei sistemi e delle reti di TI all'interno della Commissione. Il capo dell'ufficio di sicurezza della Commissione decide, d'intesa con le competenti NSA, circa l'accreditamento dei sistemi e delle reti di TI che coinvolgono la Commissione, da un lato, e qualsiasi altro destinatario di informazioni classificate UE, dall'altro.

15. ISPEZIONI DI SICUREZZA

L'ufficio di sicurezza della Commissione compie ispezioni periodiche dei dispositivi di sicurezza per la protezione delle informazioni classificate UE.

L'ufficio di sicurezza della Commissione può essere assistito, nell'esercizio di questa funzione, dai servizi di sicurezza di altre istituzioni dell'UE che custodiscono ICUE o dalle NSA degli Stati membri [1].

A richiesta di uno Stato membro, la rispettiva NSA può compiere un'ispezione di ICUE all'interno della Commissione, di comune accordo e in collaborazione con l'ufficio di sicurezza della Commissione.

[1] Fatti salvi la convenzione di Vienna del 1961 sulle relazioni diplomatiche e il protocollo sui privilegi e le immunità delle Comunità europee dell'8 aprile 1965.

16. CLASSIFICAZIONI, INDICAZIONI DI SICUREZZA E CONTRASSEGNI

16.1. Gradi di classificazione [1]

Le informazioni sono classificate con i seguenti gradi (cfr. anche appendice 2):

UE SEGRETISSIMO: questa classificazione si applica soltanto a informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare danni di eccezionale gravità agli interessi fondamentali dell'Unione europea o di uno o più Stati membri.

UE SEGRETO: questa classificazione si applica soltanto a informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gravemente gli interessi fondamentali dell'Unione europea o di uno o più Stati membri.

UE RISERVATISSIMO: questa classificazione si applica a informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gli interessi fondamentali dell'Unione europea o di uno o più Stati membri.

UE RISERVATO: questa classificazione si applica a informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare pregiudizio agli interessi dell'Unione europea o di uno o più Stati membri.

Non sono ammesse altre classificazioni.

16.2. Indicazioni di sicurezza

Possono essere utilizzate indicazioni di sicurezza convenzionali per porre limiti alla validità di una classificazione (per il declassamento o la declassificazione automatica di informazioni classificate). Tali indicazioni possono essere: «FINO A ..... (periodo/data)» o FINO A .... (evento).

Qualora risultino necessari una distribuzione limitata e un trattamento speciale oltre a quanto indicato dalla classificazione di sicurezza, si appongono indicazioni supplementari quali CRYPTO o qualunque altra indicazione di sicurezza riconosciuta a livello UE.

Le indicazioni di sicurezza possono essere utilizzate soltanto unitamente ad una classificazione.

16.3. Contrassegni

Un contrassegno può essere usato per specificare un settore che forma oggetto del documento o una distribuzione particolare sulla base del principio della necessità di sapere, ovvero per indicare il termine di un embargo (nel caso di informazioni non classificate).

Un contrassegno non è una classificazione e non deve essere usato al posto di questa.

Il contrassegno ESDP/PESD si appone su documenti e copie degli stessi concernenti la sicurezza e la difesa dell'Unione o di uno o più Stati membri o relativi alla gestione delle crisi militari o non militari.

16.4. Apposizione della classificazione

La classificazione si appone nel modo seguente:

a) su documenti UE RISERVATO con mezzi meccanici o elettronici;

b) su documenti UE RISERVATISSIMO con mezzi meccanici o a mano o a stampa su carta prestampigliata, registrata;

c) su documenti UE SEGRETO e UE SEGRETISSIMO con mezzi meccanici e a mano.

16.5. Apposizione delle indicazioni di sicurezza

Le indicazioni di sicurezza sono apposte immediatamente sotto la classificazione, con lo stesso mezzo usato per la classificazione.

[1] Nell'appendice 1 è riportata una tabella comparativa delle classificazioni di sicurezza UE, NATO, UEO e degli Stati membri.

17. GESTIONE DELLA CLASSIFICAZIONE

17.1. **Considerazioni generali**

Le informazioni sono classificate solo se necessario. La classificazione è indicata chiaramente e correttamente ed è mantenuta solo per la durata in cui è necessario proteggere l'informazione.

La responsabilità della classificazione dell'informazione e di eventuali declassamenti o declassificazioni successivi spetta unicamente all'originatore.

Il funzionario o altro agente della Commissione classifica, declassa o declassifica un'informazione su istruzione del suo superiore gerarchico o d'intesa con il medesimo.

Le modalità dettagliate per il trattamento dei documenti classificati sono state elaborate in modo da garantire che essi siano soggetti a una protezione commisurata alle informazioni che contengono.

Il numero di persone autorizzate ad emanare documenti UE SEGRETISSIMO è limitato al minimo e il loro nominativo figura in un elenco compilato dall'ufficio di sicurezza della Commissione.

17.2. **Attribuzione delle classificazioni**

La classificazione di un documento è determinata dal livello di sensibilità del suo contenuto, secondo la definizione di cui alla sezione 16. È importante che la classificazione sia attribuita correttamente e con moderazione, in particolare per quanto riguarda la classificazione UE SEGRETISSIMO.

L'originatore di un documento che deve essere classificato tiene presenti le disposizioni sopraelencate e limita la tendenza alla sovra - o sottoclassificazione.

Nell'appendice 2 figura una guida pratica per la classificazione.

È possibile che singole pagine, paragrafi, sezioni, annessi, appendici, allegati di un determinato documento e altro materiale accluso richiedano classificazioni differenti: in tal caso, all'insieme del documento viene attribuita la classificazione dell'elemento con grado più elevato.

Il grado di classificazione attribuito a una lettera o nota cui è accluso altro materiale corrisponde a quello dell'elemento accluso con grado più elevato. L'originatore indica chiaramente il grado di classificazione da attribuire alla lettera o nota quando è separata dal materiale accluso.

L'accesso del pubblico continua ad essere disciplinato dal regolamento (CE) n. 1049/2001.

17.3. **Declassamento e declassificazione**

I documenti classificati UE possono essere declassati o declassificati unicamente con il consenso dell'originatore e, se necessario, previa discussione con le altre parti interessate. Il declassamento o la declassificazione sono confermati per iscritto. L'originatore è tenuto ad informare i destinatari del cambiamento di classificazione e questi ultimi sono a loro volta tenuti ad informarne i destinatari successivi ai quali hanno trasmesso l'originale o una copia del documento.

Nella misura del possibile, l'originatore indica sul documento classificato la data, un termine o un evento a partire dal quale le informazioni in esso contenute potranno essere declassate o declassificate. In caso contrario, esso verifica almeno ogni cinque anni che la classificazione iniziale del documento sia tuttora necessaria.

18. SICUREZZA MATERIALE

18.1. **Considerazioni generali**

Scopo principale delle misure di sicurezza materiale è di evitare che le persone non autorizzate abbiano accesso alle informazioni e/o al materiale classificato UE, di prevenire il furto e la manomissione di attrezzature e altri beni, nonché di impedire che il personale o altri agenti e visitatori vengano molestati o aggrediti.

18.2. **Requisiti di sicurezza**

Tutti i locali, zone, edifici, uffici, stanze, sistemi di comunicazione e d'informazione, ecc. in cui sono custoditi e/o trattati informazioni e materiale classificati UE sono protetti da adeguate misure di sicurezza materiale.

Per la decisione sul grado di protezione materiale necessario occorre tener conto di tutti i fattori pertinenti, quali:

a) il grado di classificazione dell'informazione e/o del materiale;

b) la quantità e la forma (ad esempio supporto cartaceo, mezzi di archiviazione elettronica) delle informazioni detenute;

c) la minaccia in loco rappresentata da servizi segreti che prendono di mira l'UE, gli Stati membri e/o altre istituzioni o terzi in possesso di informazioni classificate UE, nonché segnatamente da atti di sabotaggio, terrorismo e altri atti sovversivi e/o criminali.

Le misure di sicurezza materiale applicate sono volte a:

a) impedire agli intrusi l'ingresso fraudolento o con la forza;

b) dissuadere, impedire e scoprire azioni da parte di personale in malafede;

c) impedire l'accesso a informazioni classificate UE a coloro che non hanno necessità di sapere.

18.3. **Misure di sicurezza materiale**

18.3.1. *Zone di sicurezza*

Le zone in cui sono trattate e custodite le informazioni classificate UE RISERVATISSIMO o di grado superiore sono organizzate e strutturate in modo da corrispondere a uno dei seguenti parametri:

a) zona di sicurezza di categoria I: zona in cui sono trattate e custodite informazioni UE RISERVATISSIMO o di grado superiore in modo che l'ingresso in tale zona rappresenti, a tutti i fini pratici, l'accesso alle informazioni classificate. Per tale zona occorre prevedere:

   i) un perimetro chiaramente delimitato e protetto attraverso cui controllare tutti gli ingressi e le uscite;

   ii) un sistema di controllo all'entrata che consenta l'ingresso solo alle persone in possesso di debito nulla osta di sicurezza ed espressamente autorizzate ad entrare in tale zona;

   iii) la specificazione della classificazione attribuita all'informazione normalmente custodita nella zona in questione, ossia l'informazione cui si accede entrando in tale zona;

b) zona di sicurezza di categoria II: zona in cui sono trattate e custodite informazioni UE RISERVATISSIMO o di grado superiore in modo da proteggerle dall'accesso di persone non autorizzate mediante controlli interni, ad esempio edifici in cui si trovano gli uffici in cui vengono di solito trattate e custodite le informazioni UE RISERVATISSIMO o di grado superiore. Per tale zona occorre prevedere:

   i) un perimetro chiaramente delimitato e protetto attraverso cui controllare tutti gli ingressi e le uscite;

   ii) un sistema di controllo all'entrata che consenta l'ingresso senza scorta solo alle persone in possesso di debito nulla osta di sicurezza ed espressamente autorizzate ad entrare in tale zona. Per tutte le altre persone occorre prevedere scorte o controlli equivalenti per evitare l'accesso non autorizzato alle informazioni classificate UE e l'ingresso non controllato a zone soggette a ispezioni tecniche di sicurezza.

Le zone non occupate da personale in servizio 24 ore al giorno sono ispezionate immediatamente dopo il normale orario di lavoro per garantire che le informazioni classificate UE siano correttamente protette.

18.3.2. *Zona amministrativa*

In prossimità delle zone di sicurezza di categoria I e II o per accedere a tali zone, può essere creata una zona amministrativa con minor livello di sicurezza. Occorre prevedere un perimetro chiaramente delimitato per l'ispezione del personale e dei veicoli. Nella zona amministrativa possono essere trattate e custodite solo informazioni classificate UE RISERVATO o non classificate.

18.3.3. *Controlli all'entrata e all'uscita*

L'ingresso alle zone di sicurezza delle categorie I e II è controllato da un lasciapassare o da un sistema di riconoscimento personale che si applica all'insieme del personale che presta regolarmente servizio in queste zone. È altresì predisposto un sistema di controllo dei visitatori al fine di impedire l'accesso non autorizzato ad informazioni classificate UE. I sistemi di lasciapassare possono essere completati da altri di identificazione automatizzata, senza che ciò sostituisca totalmente le guardie di sicurezza. Una modifica nella valutazione del rischio può comportare un rafforzamento delle misure di controllo delle entrate e delle uscite, per esempio durante le visite di personalità.

18.3.4. *Ronde di controllo*

Le ronde di controllo delle zone di sicurezza di categoria I e II vengono effettuate al di fuori del normale orario di lavoro per proteggere i beni dell'UE dal rischio di manomissioni, danni o perdite. Le ronde sono effettuate secondo una frequenza determinata dalle circostanze locali ma, indicativamente, ogni due ore.

18.3.5. *Contenitori di sicurezza e camere blindate*

Le informazioni classificate UE sono custodite in contenitori suddivisi in tre categorie:

— categoria A: contenitori approvati a livello nazionale per custodire informazioni classificate UE SEGRETISSIMO nelle zone di sicurezza delle categorie I e II,

— categoria B: contenitori approvati a livello nazionale per custodire informazioni classificate UE SEGRETO e UE RISERVATISSIMO nelle zone di sicurezza delle categorie I e II,

— categoria C: mobili da ufficio atti a custodire solo le informazioni classificate UE RISERVATO.

Nelle camere blindate costruite in una zona di sicurezza della categoria I o II, e in tutte le zone di sicurezza della categoria I in cui le informazioni classificate UE RISERVATISSIMO o di grado superiore sono custodite in scaffali aperti o in cui si visualizzano prospetti, piantine, ecc., le pareti, il pavimento ed il soffitto, la o le porte provviste di serratura o serrature sono omologate dalla SAA per garantire che offrano una protezione equivalente alla categoria di contenitore di sicurezza approvato per custodire informazioni con lo stesso grado di classificazione.

18.3.6. *Dispositivi di chiusura*

I dispositivi di chiusura utilizzati per i contenitori di sicurezza e le camere blindate in cui sono custodite informazioni classificate UE devono soddisfare i seguenti requisiti:

— gruppo A: approvati a livello nazionale per contenitori della categoria A,

— gruppo B: approvati a livello nazionale per contenitori della categoria B,

— gruppo C: idonei solo per i mobili da ufficio della categoria C.

18.3.7. *Controllo delle chiavi e delle combinazioni*

Le chiavi dei contenitori di sicurezza non possono essere asportate dagli edifici della Commissione. La combinazione dei contenitori di sicurezza deve essere conosciuta a memoria dalle persone che ne fanno uso. Il responsabile della sicurezza a livello locale presso il servizio interessato ha la responsabilità delle chiavi di riserva e di una traccia scritta di tutte le combinazioni, conservate in singoli plichi opachi sigillati, di cui far uso in caso di emergenza. Le chiavi, le chiavi di riserva e le combinazioni sono custodite in contenitori di sicurezza separati. Le chiavi e le combinazioni ricevono almeno la stessa protezione riservata al materiale cui danno accesso.

La combinazione dei contenitori di sicurezza è portata a conoscenza del minor numero di persone possibile. Le combinazioni vengono sostituite:

a) al ricevimento di ogni nuovo contenitore:

b) ad ogni cambiamento di personale:

c) ad ogni manomissione, effettiva o sospettata

d) ad intervalli possibilmente semestrali, e per lo meno ogni dodici mesi.

18.3.8. *Dispositivi per il rilevamento di intrusi*

Quando le informazioni classificate UE sono protette da sistemi di allarme, televisione a circuito chiuso e altri dispositivi elettrici, si prevede un'erogazione di elettricità di emergenza per garantire il funzionamento ininterrotto del sistema in caso di avaria del sistema centrale. È altresì indispensabile che in caso di disfunzione o di manomissione di detti sistemi, venga attivato un allarme o un altro segnale affidabile per il servizio di sicurezza.

18.3.9. *Attrezzatura approvata*

L'ufficio di sicurezza della Commissione mantiene elenchi aggiornati, suddivisi per tipo e modello, dell'attrezzatura di sicurezza approvata per la protezione delle informazioni classificate in varie circostanze e condizioni specificate. Questi elenchi sono compilati sulla base, tra l'altro, delle informazioni fornite dalle NSA.

18.3.10. *Protezione materiale delle fotocopiatrici e dei fax*

Le fotocopiatrici e i fax sono protetti materialmente per quanto necessario a garantire che solo le persone autorizzate possano usarli e che tutti i documenti classificati da essi prodotti siano soggetti a opportuni controlli.

18.4. **Protezione contro sguardi e ascolti indiscreti**

18.4.1. *Sguardi indiscreti*

Per garantire che le informazioni classificate UE non siano visionate, anche accidentalmente, da persone non autorizzate, devono essere prese tutte le misure appropriate, sia di giorno che di notte.

18.4.2. *Ascolti indiscreti*

Gli uffici o le zone in cui si discutono regolarmente informazioni classificate UE SEGRETO o di grado superiore sono protetti dall'ascolto indiscreto attivo e passivo qualora il rischio lo giustifichi. La valutazione del rischio di tale eventualità spetta all'ufficio di sicurezza della Commissione, eventualmente previa consultazione delle NSA.

18.4.3. *Introduzione di apparecchi elettronici e di registrazione*

È vietato introdurre telefoni cellulari, computer portatili, registratori, apparecchi fotografici e altri dispositivi elettronici o di registrazione nelle zone di sicurezza o nelle zone tecnicamente sicure senza previa autorizzazione del capo dell'ufficio di sicurezza della Commissione.

Per decidere le misure di protezione che occorre prendere nei locali che possono essere soggetti ad ascolto indiscreto passivo (per esempio, isolamento dei muri, delle porte, del pavimento e del soffitto, misurazione delle emissioni compromettenti) e all'ascolto indiscreto attivo (per esempio, ricerca di microfoni), l'ufficio di sicurezza della Commissione può chiedere l'assistenza di esperti delle NSA.

Parimenti, su richiesta del capo dell'ufficio di sicurezza, quando le circostanze lo rendano necessario, specialisti della sicurezza tecnica delle NSA possono ispezionare il materiale per le telecomunicazioni e qualsiasi tipo di attrezzatura elettrica o elettronica da ufficio utilizzata durante le riunioni di livello UE SEGRETO e di grado superiore.

18.5. **Zone tecnicamente sicure**

Talune zone possono essere designate come «zone tecnicamente sicure». Per queste zone è previsto un controllo speciale all'ingresso. Quando non vengono occupate, tali zone sono chiuse a chiave mediante una procedura convenuta, e tutte le chiavi sono considerate chiavi di sicurezza. Queste zone sono soggette a regolari ispezioni materiali, cui si procederà anche dopo ogni ingresso non autorizzato, effettivo o sospettato.

Si procede ad un inventario particolareggiato dell'attrezzatura e dei mobili per controllarne la movimentazione. In queste zone non possono essere introdotti mobili o altra attrezzatura che non siano stati precedentemente verificati con cura dal personale di sicurezza avente una formazione specifica per rilevare qualsiasi meccanismo di ascolto. Come regola generale, nelle zone tecnicamente sicure è vietato installare linee di comunicazione, salvo previa autorizzazione da parte dell'autorità competente.

19. REGOLE GENERALI RELATIVE AL PRINCIPIO DELLA NECESSITÀ DI SAPERE E AL NULLA OSTA DI SICUREZZA

19.1. Considerazioni generali

L'accesso alle ICUE è consentito solo alle persone che hanno «necessità di sapere» per lo svolgimento delle loro funzioni o missioni. L'accesso alle informazioni UE SEGRETISSIMO, UE SEGRETO e UE RISERVATISSIMO è autorizzato solo per le persone in possesso dell'apposito nulla osta di sicurezza.

La responsabilità di determinare la «necessità di sapere» spetta al capo del servizio presso il quale l'interessato deve lavorare.

Spetta a ciascun servizio fare richiesta di nulla osta per il proprio personale.

Tale procedura si conclude con il rilascio di un «nulla osta di sicurezza» in cui è specificato il grado di classificazione delle informazioni cui la persona abilitata ha accesso e la data di scadenza di tale nulla osta.

Un nulla osta di sicurezza per un determinato grado di classificazione può conferire al titolare il diritto di accesso ad informazioni classificate di grado inferiore.

Le persone che non sono funzionari o altri agenti delle istituzioni dell'UE, quali ad esempio contraenti, esperti o consulenti con cui possa essere necessario discutere informazioni classificate UE, o ai quali tali informazioni debbano essere mostrate, devono possedere un nulla osta di sicurezza per le informazioni classificate UE ed essere istruite quanto alla loro responsabilità in materia di sicurezza.

L'accesso del pubblico continua ad essere disciplinato dal regolamento (CE) n. 1049/2001.

19.2. Regole particolari sull'accesso alle informazioni UE SEGRETISSIMO

La persona che deve accedere ad informazioni UE SEGRETISSIMO vi è autorizzata solo previa indagine.

La persona che deve accedere ad informazioni UE SEGRETISSIMO è designata dal membro della Commissione competente in materia di sicurezza e il suo nominativo è inserito nell'apposito registro UE SEGRETISSIMO. Tale registro è compilato e tenuto dall'ufficio di sicurezza della Commissione.

Prima di accedere alle informazioni UE SEGRETISSIMO, la persona in questione deve firmare un certificato in cui dichiara di essere stata istruita sulle procedure della Commissione in materia di sicurezza e di essere pienamente consapevole della responsabilità che le incombe quanto alla protezione delle informazioni UE SEGRETISSIMO nonché delle conseguenze previste dalle norme UE e dalle norme legislative o amministrative nazionali qualora informazioni classificate vengano divulgate a persone non autorizzate, intenzionalmente o per negligenza.

Per le persone che hanno accesso a informazioni UE SEGRETISSIMO nel corso di riunioni, ecc., il funzionario di controllo competente del servizio o dell'organismo presso il quale dette persone sono assunte notifica all'organizzatore della riunione che le persone in questione sono debitamente autorizzate a parteciparvi.

Il nominativo della persona che cessi di svolgere funzioni per le quali è richiesto l'accesso ad informazioni UE SEGRETISSIMO è rimosso dall'elenco UE SEGRETISSIMO. Inoltre, la sua attenzione è nuovamente richiamata sulla responsabilità particolare che le incombe quanto alla protezione delle informazioni UE SEGRETISSIMO. Essa è anche tenuta a firmare una dichiarazione in cui si impegna a non utilizzare o divulgare le informazioni UE SEGRETISSIMO in suo possesso.

19.3. Regole particolari sull'accesso alle informazioni UE SEGRETO e UE RISERVATISSIMO

La persona che deve accedere ad informazioni UE SEGRETO e UE RISERVATISSIMO vi è autorizzata solo previa indagine.

La persona che deve accedere ad informazioni UE SEGRETO e UE RISERVATISSIMO deve essere a conoscenza delle pertinenti norme di sicurezza ed essere consapevole delle conseguenze di un atto di negligenza.

Per le persone che hanno accesso ad informazioni UE SEGRETO e UE RISERVATISSIMO nel corso di riunioni, ecc., il funzionario di controllo competente del servizio o dell'organismo presso il quale dette persone sono assunte notifica all'organizzatore della riunione che le persone in questione sono debitamente autorizzate a parteciparvi.

19.4. Regole particolari sull'accesso alle informazioni UE RISERVATO

La persona che ha accesso ad informazioni UE RISERVATO viene messa a conoscenza delle presenti norme di sicurezza e delle conseguenze di un atto di negligenza.

19.5. Trasferimenti

Quando un membro del personale è trasferito da un posto che comporta il trattamento di materiale classificato UE, l'ufficio di registrazione provvede al corretto trasferimento di detto materiale dal funzionario uscente al funzionario entrante.

Quando un membro del personale è trasferito ad un altro posto che comporta il trattamento di materiale classificato UE, il responsabile della sicurezza a livello locale provvede ad impartirgli le debite istruzioni.

19.6. Istruzioni particolari

La persona che deve trattare informazioni classificate UE deve essere messa a conoscenza, all'atto dell'assunzione e successivamente con periodicità, di quanto segue:

a) i pericoli per la sicurezza derivanti da conversazioni indiscrete;

b) le precauzioni da prendere nei rapporti con la stampa e con rappresentanti di particolari gruppi d'interessi;

c) la minaccia rappresentata dalle attività di servizi segreti che prendono di mira l'UE e gli Stati membri per quanto riguarda le informazioni e le attività classificate UE;

d) l'obbligo di riferire immediatamente alle competenti autorità di sicurezza in merito a qualsiasi approccio o manovra che possa destare sospetti su un'eventuale attività di spionaggio o a qualsiasi circostanza inabituale in fatto di sicurezza.

Tutti coloro che sono abitualmente esposti a frequenti contatti con rappresentanti di paesi i cui servizi segreti prendono di mira l'UE e gli Stati membri per quanto riguarda le informazioni e le attività classificate UE vengono istruiti sulle tecniche notoriamente impiegate dai vari servizi segreti.

Non esistono norme di sicurezza della Commissione per quanto riguarda i viaggi personali verso qualsiasi destinazione effettuati da personale abilitato all'accesso a informazioni classificate UE. L'ufficio di sicurezza della Commissione, tuttavia, informa i funzionari e altri agenti di cui è responsabile in merito alle disposizioni in materia di viaggio cui possono essere soggetti.

20. PROCEDURA PER IL RILASCIO DEL NULLA OSTA DI SICUREZZA AI FUNZIONARI E ALTRI AGENTI DELLA COMMISSIONE

a) Hanno accesso alle informazioni classificate in possesso della Commissione soltanto i funzionari e gli altri agenti della Commissione o le persone che lavorano in seno alla Commissione che, a motivo delle loro funzioni e per esigenze di servizio, abbiano bisogno di prenderne visione o di effettuarne il trattamento.

b) Per poter accedere alle informazioni classificate UE SEGRETISSIMO, UE SEGRETO e UE RISERVATISSIMO, le persone di cui alla lettera a) devono essere state autorizzate a tal fine secondo la procedura di cui alle lettere c) e d) della presente sezione.

c) Il nulla osta di sicurezza è rilasciato soltanto alle persone che sono state oggetto di un'indagine di sicurezza da parte delle autorità nazionali competenti degli Stati membri (NSA) secondo la procedura di cui alle lettere da i) a n).

d) Il capo dell'ufficio di sicurezza della Commissione è competente per il rilascio del nulla osta di sicurezza di cui alle lettere a), b) e c).

e) Il capo dell'ufficio di sicurezza della Commissione rilascia tale nulla osta previo parere delle autorità nazionali competenti degli Stati membri sulla base dell'indagine di sicurezza condotta conformemente alle lettere da i) a n).

f) L'ufficio di sicurezza della Commissione tiene un elenco aggiornato di tutti i posti sensibili, comunicati dai rispettivi servizi della Commissione, e di tutte le persone cui è stato rilasciato un nulla osta di sicurezza (temporaneo).

g) Il nulla osta di sicurezza, che è valido per un periodo di cinque anni, non può avere durata superiore a quella delle funzioni che ne hanno giustificato il rilascio. Esso può essere rinnovato secondo la procedura di cui alla lettera e).

h) Il nulla osta di sicurezza è revocato dal capo dell'ufficio di sicurezza della Commissione ove questi ritenga che ve ne sia fondato motivo. La decisione di revoca è notificata alla persona interessata, che può chiedere di essere ascoltata dal capo dell'ufficio di sicurezza della Commissione, nonché all'autorità nazionale competente.

i) L'indagine di sicurezza è effettuata, con la collaborazione della persona interessata e su richiesta del capo dell'ufficio di sicurezza della Commissione, dalle autorità nazionali competenti dello Stato membro di cui l'interessato è cittadino. Se la persona interessata non ha la cittadinanza di uno Stato membro dell'UE, il capo dell'ufficio di sicurezza della Commissione chiede che a svolgere l'indagine di sicurezza sia lo Stato membro dell'UE in cui l'interessato ha eletto domicilio o risiede abitualmente.

j) Ai fini dell'indagine la persona interessata è tenuta a compilare un modulo informativo individuale.

k) Nella richiesta il capo dell'ufficio di sicurezza della Commissione specifica il tipo e il grado di classificazione delle informazioni a cui la persona interessata dovrà accedere, per consentire alle autorità nazionali competenti di svolgere l'indagine ed esprimere un parere relativamente al grado di abilitazione da rilasciare alla persona in questione.

l) Sia lo svolgimento che i risultati della procedura d'indagine sono soggetti alle pertinenti disposizioni legislative e amministrative vigenti nello Stato membro interessato, comprese quelle relative agli eventuali mezzi di impugnazione.

m) Se le autorità nazionali competenti degli Stati membri esprimono parere positivo, il capo dell'ufficio di sicurezza della Commissione può rilasciare il nulla osta alla persona interessata.

n) Se le autorità nazionali competenti esprimono parere negativo, la persona interessata è informata di tale parere e può chiedere di essere ascoltata dal capo dell'ufficio di sicurezza della Commissione. Il capo dell'ufficio di sicurezza della Commissione può, se lo ritiene necessario, rivolgersi alle autorità nazionali competenti per chiedere i chiarimenti complementari che siano in grado di fornire. In caso di riconferma del parere negativo, il nulla osta non può essere rilasciato.

o) Ogni persona che abbia ottenuto il nulla osta a norma delle lettere d) ed e) riceve, al momento del rilascio del medesimo e successivamente ad intervalli regolari, le necessarie istruzioni concernenti la protezione delle informazioni classificate e le modalità per garantirla. Essa firma una dichiarazione in cui conferma di avere ricevuto tali istruzioni e di impegnarsi a rispettarle.

p) Il capo dell'ufficio di sicurezza della Commissione adotta le misure necessarie per attuare le disposizioni della presente sezione, in particolare per quanto riguarda le norme in materia di accesso all'elenco delle persone abilitate.

q) In via eccezionale e per esigenze di servizio, il capo dell'ufficio di sicurezza della Commissione, previa notificazione delle autorità nazionali competenti e in mancanza di reazioni da parte di queste ultime entro il termine di un mese, può rilasciare un nulla osta a titolo temporaneo per un periodo non superiore a sei mesi, in attesa dell'esito dell'indagine di cui alla lettera i).

r) I nulla osta provvisori e temporanei rilasciati non danno accesso alle informazioni UE SEGRETISSIMO: tale accesso è limitato ai funzionari che siano stati effettivamente sottoposti a un'indagine di sicurezza con esito positivo, ai sensi della lettera i). In attesa dell'esito dell'indagine, i funzionari per i quali è stato richiesto un nulla osta di sicurezza al grado UE SEGRETISSIMO possono essere abilitati in via temporanea e provvisoria ad accedere a informazioni classificate fino al grado UE SEGRETO incluso.

21. ELABORAZIONE, DISTRIBUZIONE, TRASMISSIONE, SICUREZZA DEL PERSONALE DEI CORRIERI, COPIE, TRADUZIONI ED ESTRATTI DI DOCUMENTI CLASSIFICATI UE

21.1. Elaborazione

1. Le classificazioni UE sono apposte secondo le disposizioni della sezione 16: le classificazioni UE RISERVATISSIMO e di grado superiore figurano sulla parte superiore e inferiore di ogni pagina, al centro: ogni pagina è numerata. Ciascun documento classificato UE reca un numero di riferimento e una data. Nei documenti UE SEGRETISSIMO e UE SEGRETO il numero di riferimento figura su ciascuna pagina. Qualora i documenti siano distribuiti in più esemplari, ognuno di essi reca un numero di copia che figura sulla prima pagina, a fianco del numero totale di pagine. Tutti gli allegati e il materiale accluso sono elencati sulla prima pagina dei documenti classificati UE RISERVATISSIMO o di grado superiore.

2. I documenti classificati UE RISERVATISSIMO o di grado superiore sono dattiloscritti, tradotti, archiviati, fotocopiati, riprodotti su supporto magnetico o microfilm soltanto da persone che hanno ricevuto il nulla osta di sicurezza per l'accesso alle informazioni classificate UE per un grado almeno pari alla classificazione di sicurezza del documento in questione.

3. Le disposizioni che disciplinano la produzione informatica di documenti classificati sono riportate nella sezione 25.

21.2. **Distribuzione**

1. Le informazioni classificate UE sono distribuite solo alle persone aventi necessità di sapere e che hanno ricevuto l'apposito nulla osta di sicurezza. La distribuzione iniziale è specificata dall'originatore.

2. I documenti UE SEGRETISSIMO sono distribuiti tramite gli uffici di registrazione UE SEGRETISSIMO (cfr. punto 22.2). Per i messaggi UE SEGRETISSIMO l'ufficio di registrazione competente può autorizzare il responsabile del centro di comunicazioni a produrre il numero di copie specificato nell'elenco dei destinatari.

3. I documenti classificati UE SEGRETO o di grado inferiore possono essere ridistribuiti dal destinatario iniziale ad altri destinatari in base alla necessità di sapere. Le autorità d'origine tuttavia indicano chiaramente ogni limitazione che desiderano imporre. In presenza di tali limitazioni i destinatari possono ridistribuire i documenti solo con l'autorizzazione dell'autorità d'origine.

4. Ogni documento classificato UE RISERVATISSIMO o di grado superiore viene registrato, all'entrata e all'uscita dalla DG o dal servizio, dall'ufficio di registrazione locale. I dettagli da annotare (riferimenti, data e, se del caso, numero della copia) sono tali da consentire l'identificazione dei documenti e sono iscritti in un repertorio o registrati su un supporto informatico appositamente protetto (cfr. punto 22.1).

21.3. **Trasmissione di documenti classificati UE**

21.3.1. *Plico, ricevuta*

1. I documenti classificati UE RISERVATISSIMO o di grado superiore sono trasmessi in buste doppie, resistenti, opache. La busta interna reca la pertinente classificazione di sicurezza UE e, ove possibile, i dati completi della funzione, del titolo e dell'indirizzo del destinatario.

2. Solo il funzionario di controllo dell'ufficio di registrazione (cfr. punto 22.1), o il suo sostituto, può aprire la busta interna e accusare ricevuta dei documenti che contiene, a meno che essa sia indirizzata ad una persona determinata. In tal caso il competente ufficio di registrazione (cfr. punto 22.1) registra l'entrata della busta e soltanto la persona cui essa è indirizzata può aprire la busta interna e accusare ricevuta dei documenti in essa contenuti.

3. Nella busta interna viene inserito un modulo di ricevuta, che non viene classificato, indicante il numero di riferimento, la data e il numero di copia del documento ma in nessun caso l'oggetto del contenuto.

4. La busta interna è inserita in una busta esterna recante un numero di plico ai fini della ricevuta. In nessun caso la busta esterna reca la classificazione di sicurezza.

5. Per i documenti classificati UE RISERVATISSIMO o di grado superiore, viene consegnata al messo una ricevuta con il numero di plico.

21.3.2. *Trasmissione all'interno di un edificio o di un gruppo di edifici*

All'interno di un determinato edificio o gruppo di edifici, i documenti classificati possono essere trasportati in una busta sigillata recante unicamente il nome del destinatario, purché il trasporto sia effettuato direttamente da una persona abilitata al grado di classificazione dei documenti.

21.3.3. *Trasmissione all'interno di un paese*

1. All'interno di un paese i documenti UE SEGRETISSIMO devono essere inviati solo per mezzo di un servizio ufficiale di messaggeria o tramite persone autorizzate ad accedere ad informazioni UE SEGRETISSIMO.

2. Per il ricorso a un servizio di messaggeria in caso di trasmissione di un documento UE SEGRETISSIMO al di fuori di un edificio o di un gruppo di edifici, devono essere rispettate le disposizioni relative al plico e alla ricezione di cui al presente capitolo. L'organico dei servizi di messaggeria dev'essere tale da garantire che i plichi contenenti documenti UE SEGRETISSIMO siano in ogni momento sotto la supervisione diretta di un funzionario responsabile.

3. In via eccezionale i documenti UE SEGRETISSIMO possono essere trasportati da funzionari, non appartenenti a un servizio di messaggeria, al di fuori di un edificio o gruppo di edifici per la loro utilizzazione in loco nel corso di riunioni o discussioni, purché:

   a) il latore sia abilitato ad accedere a documenti UE SEGRETISSIMO;

   b) il modo di trasporto sia conforme alle norme nazionali che disciplinano la trasmissione di documenti nazionali «segretissimi»;

   c) in nessuna circostanza i documenti UE SEGRETISSIMO siano lasciati incustoditi;

   d) si prendano disposizioni affinché l'elenco dei documenti trasportati in tal modo sia iscritto presso l'ufficio di registrazione UE SEGRETISSIMO che detiene i documenti e in un apposito repertorio e sia ricontrollato all'atto della riconsegna.

4. All'interno di un paese, i documenti UE SEGRETO e UE RISERVATISSIMO possono essere spediti sia per posta, se tale tipo di trasmissione è consentita in base alle norme nazionali ed è conforme a dette norme, o tramite servizio di messaggeria oppure affidandoli a persone abilitate all'accesso alle informazioni classificate UE.

5. L'ufficio di sicurezza della Commissione elabora istruzioni per il personale che trasporta documenti classificati UE in base alle presenti norme. Il latore è tenuto a leggere e firmare tali istruzioni, le quali stabiliscono, in particolare, che in nessun caso i documenti:

   a) siano lasciati dal latore, a meno che siano custoditi in modo sicuro ai sensi delle disposizioni della sezione 18;

   b) siano lasciati incustoditi su mezzi di trasporto pubblico o all'interno di veicoli privati, o in luoghi quali ristoranti o alberghi. Essi non possono essere depositati nella cassaforte degli alberghi o restare incustoditi nelle camere;

   c) siano letti in luoghi pubblici quali aeromobili e treni.

21.3.4. *Trasmissione da uno Stato all'altro*

1. Il materiale classificato UE RISERVATISSIMO o di grado superiore è trasferito mediante valigia diplomatica o corriere militare.

2. Tuttavia il trasporto personale di materiale classificato UE SEGRETO e UE RISERVATISSIMO è consentito se le modalità di trasporto sono tali da garantire che detto materiale non possa cadere nelle mani di persone non autorizzate.

3. Il membro della Commissione competente in materia di sicurezza può autorizzare il trasporto personale quando la valigia diplomatica e il corriere militare non siano disponibili o quando il ricorso a tali mezzi di trasporto comporti un ritardo che sarebbe dannoso per le operazioni dell'UE, nonché quando il materiale sia richiesto urgentemente dal destinatario designato. L'ufficio di sicurezza della Commissione prepara istruzioni per il trasporto personale internazionale di materiale classificato fino al grado di UE SEGRETO incluso, effettuato da persone che non siano corrieri diplomatici o militari. Ai sensi di tali istruzioni:

   a) il latore deve avere il pertinente nulla osta di sicurezza;

   b) il materiale trasportato è registrato nel competente servizio o ufficio di registrazione;

   c) i plichi o le valigie contenenti materiale UE recano un sigillo ufficiale onde evitare o scoraggiare un'ispezione doganale, nonché etichette con l'identificazione e istruzioni per chi ritrova il materiale;

   d) il latore è munito di un certificato di corriere e/o di un ordine di missione, riconosciuto da tutti gli Stati dell'UE che lo autorizza a trasportare il plico specificato;

   e) in caso di viaggio via terra non viene attraversato alcun paese terzo, né la sua frontiera, a meno che lo Stato di spedizione non abbia ottenuto una garanzia speciale da parte del paese in questione;

   f) l'organizzazione del viaggio del latore per quanto concerne destinazioni, itinerari e mezzi di trasporto è conforme alle norme dell'UE o alle norme nazionali in materia qualora queste siano più rigorose;

g) il materiale deve sempre essere detenuto dal latore, a meno che sia custodito ai sensi delle disposizioni relative alla conservazione in luogo sicuro di cui alla sezione 18;

h) il materiale non deve essere lasciato incustodito in veicoli pubblici o privati o in luoghi quali ristoranti o alberghi. Esso non deve essere depositato nella cassaforte degli alberghi o restare incustodito nelle camere;

i) se il materiale trasportato contiene documenti, questi non devono essere letti in luoghi pubblici (ad esempio aerei, treni, ecc.).

4. La persona addetta al trasporto del materiale classificato deve leggere e firmare un documento recante istruzioni di sicurezza in cui figurino almeno le istruzioni di cui sopra e le procedure da seguire in caso di emergenza o qualora il plico contenente il materiale classificato sia richiesto per accertamenti dai servizi doganali o di sicurezza degli aeroporti.

21.3.5. *Trasmissione di documenti classificati* UE RISERVATO

Non sono previste disposizioni speciali per il trasporto di documenti UE RISERVATO, eccetto per quanto riguarda la garanzia che non cadano nelle mani di persone non autorizzate.

21.4. Sicurezza del personale dei corrieri

Tutto il personale dei servizi di corriere e di messaggeria addetto al trasporto di documenti UE SEGRETO e UE RISERVATISSIMO deve essere in possesso del pertinente nulla osta di sicurezza.

21.5. Trasmissione elettronica e altri mezzi di trasmissione tecnica

1. Le misure di sicurezza delle comunicazioni sono destinate a garantire la trasmissione sicura delle informazioni classificate UE. Le norme particolareggiate applicabili alla trasmissione di tali informazioni classificate UE figurano nella sezione 25.

2. Le informazioni classificate UE RISERVATISSIMO e UE SEGRETO possono transitare solo attraverso centri e reti di comunicazione e/o terminali e sistemi accreditati.

21.6. Esemplari supplementari, traduzioni ed estratti di documenti classificati UE

1. Solo l'originatore può autorizzare la tiratura o la traduzione di documenti UE SEGRETISSIMO.

2. Se persone che non hanno il nulla osta di sicurezza del grado UE SEGRETISSIMO richiedono informazioni le quali, sebbene contenute in un documento UE SEGRETISSIMO, non hanno tale grado di classificazione, il responsabile dell'ufficio di registrazione UE SEGRETISSIMO (cfr. punto 22.2) può essere autorizzato a produrre il numero necessario di estratti dal documento in questione. Contemporaneamente egli prende le disposizioni necessarie affinché a tali estratti venga attribuita la pertinente classificazione di sicurezza.

3. I documenti classificati UE SEGRETO o di grado inferiore possono essere riprodotti e tradotti dal destinatario nell'ambito delle presenti disposizioni e purché sia rigorosamente rispettato il principio della necessità di sapere. Le misure di sicurezza applicabili al documento originale si applicano anche alle riproduzioni e/o traduzioni del medesimo.

22. UFFICI DI REGISTRAZIONE DELLE INFORMAZIONI CLASSIFICATE UE, RASSEGNE, CONTROLLI, ARCHIVIAZIONE E DISTRUZIONE DELLE INFORMAZIONI CLASSIFICATE UE

22.1. Uffici locali di registrazione ICUE (Informazioni classificate UE)

1. In ogni servizio della Commissione uno o, se necessario, più uffici locali di registrazione ICUE sono responsabili della registrazione, riproduzione, spedizione, archiviazione e distruzione dei documenti classificati UE SEGRETO e UE RISERVATISSIMO.

2. Qualora un servizio non disponga di un ufficio locale di registrazione ICUE, tale ruolo viene svolto dall'ufficio locale del Segretariato generale.

3. Gli uffici locali di registrazione ICUE riferiscono al capo servizio da cui ricevono le istruzioni. A capo degli uffici è il funzionario di controllo dell'ufficio di registrazione (RCO).

4. Gli uffici di registrazione sono soggetti alla supervisione del responsabile locale della sicurezza per quanto attiene all'applicazione delle disposizioni sul trattamento dei documenti ICUE e al rispetto delle pertinenti misure di sicurezza.

5. I funzionari destinati agli uffici locali di registrazione ICUE devono essere abilitati ad accedere a tali documenti conformemente alla sezione 20.

6. Sotto la direzione del capo servizio competente, gli uffici locali di registrazione ICUE devono:

   a) gestire le operazioni relative alla registrazione riproduzione, traduzione, trasmissione, spedizione e distruzione di tali informazioni;

   b) aggiornare l'elenco dei dati relativi alle informazioni classificate;

   c) interrogare periodicamente gli originatori sulla necessità di mantenere la classificazione delle informazioni;

7. Gli uffici locali di registrazione ICUE tengono un registro con i seguenti dati:

   a) data di elaborazione delle informazioni classificate;

   b) grado di classificazione;

   c) data di scadenza della classificazione;

   d) nome e servizio dell'originatore;

   e) destinatario o destinatari con numero di serie;

   f) oggetto;

   g) numero;

   h) numero di esemplari distribuiti;

   i) preparazione di inventari delle informazioni classificate sottoposte al servizio;

   j) registro della declassificazione o declassamento delle informazioni classificate.

8. Le norme generali di cui alla sezione 21 si applicano agli uffici locali di registrazione ICUE della Commissione, salvo altrimenti previsto da norme specifiche della presente sezione.

22.2. L'ufficio di registrazione UE SEGRETISSIMO

22.2.1. *Considerazioni generali*

1. Un ufficio centrale di registrazione UE SEGRETISSIMO assicura che i documenti UE SEGRETISSIMO siano registrati, trattati e diffusi conformemente alle presenti norme di sicurezza. A capo dell'ufficio di registrazione UE SEGRETISSIMO è il funzionario di controllo dell'ufficio di registrazione UE SEGRETISSIMO.

2. L'ufficio centrale di registrazione UE SEGRETISSIMO è la principale autorità della Commissione preposta alla ricezione e all'invio e il referente di altre istituzioni della UE, degli Stati membri, delle organizzazioni internazionali e dei paesi terzi con cui la Commissione ha concluso accordi sulle procedure di sicurezza per lo scambio di informazioni classificate.

3. Se necessario sono istituite sottosezioni degli uffici di registrazione per la gestione interna dei documenti UE SEGRETISSIMO; tali sottosezioni dispongono di dati aggiornati relativi alla circolazione di ciascun documento di loro competenza.

4. Le sottosezioni degli uffici di registrazione UE SEGRETISSIMO sono istituite secondo le modalità di cui alla sezione 22.2.3 per far fronte a esigenze di lungo termine e sono aggregate a un ufficio centrale di registrazione UE SEGRETISSIMO. Qualora debbano essere consultati solo in via temporanea o occasionale, i documenti UE SEGRETISSIMO possono essere rilasciati senza istituire una sottosezione UE SEGRETISSIMO, purché vengano stabilite norme atte a garantire che essi rimangano sotto il controllo del competente ufficio di registrazione UE SEGRETISSIMO e che siano osservate tutte le misure di sicurezza materiali e relative al personale.

5. Le sottosezioni degli uffici di registrazione non possono trasmettere documenti UE SEGRETISSIMO direttamente ad altre sottosezioni dello stesso ufficio centrale di registrazione UE SEGRETISSIMO senza l'esplicito accordo di quest'ultimo.

6. Tutti gli scambi di documenti UE SEGRETISSIMO fra sottosezioni non aggregate allo stesso ufficio centrale di registrazione avvengono tramite gli uffici centrali di registrazione UE SEGRETISSIMO.

22.2.2. *L'ufficio centrale di registrazione UE SEGRETISSIMO*

In qualità di funzionario di controllo, il capo di un ufficio centrale di registrazione UE SEGRETISSIMO è responsabile:

a) della trasmissione di documenti UE SEGRETISSIMO conformemente alle disposizioni di cui alla sezione 21.3;

b) della compilazione di un elenco di tutte le sottosezioni dell'ufficio di registrazione UE SEGRETISSIMO che dipendono dal suo ufficio, corredato dei nomi e delle firme dei funzionari di controllo designati e dei loro supplenti autorizzati;

c) della conservazione delle ricevute dei registri per tutti i documenti UE SEGRETISSIMO distribuiti dall'ufficio centrale di registrazione;

d) della registrazione di tutti i documenti UE SEGRETISSIMO custoditi e distribuiti;

e) dell'aggiornamento costante di un elenco di tutti gli uffici centrali di registrazione UE SEGRETISSIMO con cui è normalmente in contatto, corredato dei nomi e delle firme dei rispettivi funzionari di controllo designati e dei loro supplenti autorizzati;

f) della protezione materiale di tutti i documenti UE SEGRETISSIMO custoditi presso l'ufficio di registrazione conformemente alle disposizioni di cui alla sezione 18.

22.2.3. *Sottosezioni dell'ufficio di registrazione UE SEGRETISSIMO*

In qualità di funzionario di controllo, il capo di una sottosezione dell'ufficio di registrazione UE SEGRETISSIMO è responsabile:

a) della trasmissione di documenti UE SEGRETISSIMO conformemente alle disposizioni di cui alla sezione 21.3;

b) dell'aggiornamento costante di un elenco di tutte le persone autorizzate ad accedere alle informazioni UE SEGRETISSIMO di sua competenza;

c) della distribuzione di documenti UE SEGRETISSIMO secondo le istruzioni dell'originatore o in base al principio della necessità di sapere dopo avere accertato che il destinatario sia fornito del necessario nullaosta di sicurezza;

d) dell'aggiornamento costante di un registro di tutti i documenti UE SEGRETISSIMO custoditi o circolanti sotto il suo controllo o passati ad altri uffici di registrazione UE SEGRETISSIMO e conservazione delle relative ricevute;

e) dell'aggiornamento costante dell'elenco degli uffici centrali di registrazione UE SEGRETISSIMO con cui è autorizzato a scambiare documenti UE SEGRETISSIMO, corredato dei nomi e delle firme dei rispettivi funzionari di controllo e dei loro supplenti autorizzati;

f) della protezione materiale di tutti i documenti UE SEGRETISSIMO custoditi presso la sottosezione dell'ufficio di registrazione conformemente alle disposizioni di cui alla sezione 18.

22.3. **Inventari, rassegne e controlli dei documenti classificati UE**

1. Ogni anno ogni ufficio di registrazione UE SEGRETISSIMO, di cui alla presente sezione, effettua un inventario particolareggiato dei documenti UE SEGRETISSIMO. Un documento si considera inventariato quando l'ufficio lo detiene materialmente ovvero è in possesso della ricevuta dell'ufficio di registrazione UE SEGRETISSIMO in cui il documento è stato trasferito o del certificato di distruzione del documento stesso o di istruzioni relative al suo declassamento o alla sua declassificazione. I risultati degli inventari annuali sono trasmessi al membro della Commissione responsabile per le questioni della sicurezza entro, al più tardi, il 1° aprile di ogni anno.

2. Le sottosezioni degli uffici di registrazione UE SEGRETISSIMO trasmettono i risultati dell'inventario annuale all'ufficio centrale di registrazione da cui dipendono in data stabilita da detto ufficio.

3. I documenti classificati UE di grado inferiore a UE SEGRETISSIMO sono soggetti a controlli interni in conformità delle istruzioni del membro della Commissione responsabile per le questioni della sicurezza.

4. Tali operazioni mirano ad ottenere il parere dei detentori dei documenti quanto:

   a) alla possibilità di declassare o declassificare determinati documenti;

   b) ai documenti da distruggere.

22.4. **Archiviazione delle informazioni classificate UE**

1. Le ICUE sono archiviate nel rispetto delle pertinenti disposizioni di cui alla sezione 18.

2. Al fine di ridurre al minimo i problemi di archiviazione, i funzionari di controllo di tutti gli uffici di registrazione sono autorizzati a far microfilmare i documenti UE SEGRETISSIMO, UE SEGRETO e UE RISERVATISSIMO o a farli riprodurre su supporto magnetico o ottico a fini di archiviazione, purché:

   a) il processo di trasferimento su microfilm/di archiviazione sia effettuato da personale con nulla osta valido per il corrispondente grado di classificazione;

   b) il microfilm/mezzo di archiviazione goda della stessa sicurezza dei documenti originali;

   c) il trasferimento su microfilm/l'archiviazione di ogni documento UE SEGRETISSIMO sia comunicato all'originatore;

   d) i rotoli di pellicola, o gli altri tipi di supporto, contengano solo documenti del medesimo grado di classificazione UE SEGRETISSIMO, UE SEGRETO o UE RISERVATISSIMO;

   e) il trasferimento su microfilm/l'archiviazione di un documento UE SEGRETISSIMO o UE SEGRETO sia chiaramente indicato nel registro usato per l'inventario annuale;

   f) i documenti originali che sono stati trasferiti su microfilm o archiviati in altro modo siano distrutti, conformemente alle disposizioni di cui alla sezione 22.5.

3. Queste norme si applicano altresì a qualsiasi altra forma di archiviazione autorizzata, quali i mezzi elettromagnetici e i dischi ottici.

22.5. **Distruzione di documenti classificati UE**

1. Per evitare l'accumulazione superflua di documenti classificati UE, gli esemplari che il capo dell'istituzione che li detiene considera superati o in soprannumero sono distrutti non appena possibile, nel seguente modo:

   a) i documenti UE SEGRETISSIMO sono distrutti soltanto dall'ufficio centrale di registrazione che ne è responsabile. Ogni documento distrutto viene elencato in un certificato di distruzione, firmato dal funzionario di controllo UE SEGRETISSIMO e dal funzionario che assiste alla distruzione il quale deve avere il nulla osta di sicurezza di grado UE SEGRETISSIMO. A tal fine nel repertorio viene inserita una nota.

   b) L'ufficio di registrazione tiene i certificati di distruzione, unitamente alle schede di distribuzione, per un periodo di dieci anni e ne invia copie all'originatore o al pertinente ufficio centrale di registrazione solo su richiesta esplicita.

   c) I documenti UE SEGRETISSIMO, inclusi quelli classificati e poi scartati nella fase di preparazione di documenti UE SEGRETISSIMO, quali copie rovinate, bozze di lavoro, note dattiloscritte, floppy disk devono essere distrutti sotto la sorveglianza di un funzionario di controllo dell'ufficio di registrazione UE SEGRETISSIMO mediante incenerimento o devono essere ridotti in pasta, sminuzzati o altrimenti ridotti in una forma irriconoscibile e non ricostituibile.

2. I documenti UE SEGRETO sono distrutti dall'ufficio di registrazione che ne è responsabile, sotto la sorveglianza di una persona con nulla osta di sicurezza, utilizzando uno dei processi di cui al paragrafo 1, lettera c). I documenti UE SEGRETO distrutti sono elencati in un certificato di distruzione firmato, detenuto dall'ufficio di registrazione, unitamente alle schede di distribuzione, per almeno tre anni.

3. I documenti UE RISERVATISSIMO sono distrutti dall'ufficio di registrazione che ne è responsabile, sotto la sorveglianza di una persona con nulla osta di sicurezza, utilizzando uno dei processi di cui al paragrafo 1, lettera c). La loro distruzione è registrata conformemente alle istruzioni del membro della Commissione responsabile per le questioni della sicurezza.

4. I documenti UE RISERVATO sono distrutti dall'ufficio di registrazione che ne è responsabile o dall'utente, conformemente alle istruzioni del membro della Commissione responsabile per le questioni della sicurezza.

22.6. **Distruzione in situazioni di emergenza**

1. I servizi della Commissione predispongono piani, in base alle condizioni vigenti in loco, per la protezione del materiale classificato UE in situazioni di crisi, compresa, se necessaria, la distruzione di emergenza e piani di evacuazione. Essi emanano le istruzioni che ritengono necessarie per impedire che informazioni classificate UE cadano nelle mani di persone non autorizzate.

2. Le disposizioni per la protezione e/o la distruzione di materiale UE SEGRETO e UE RISERVATISSIMO in situazioni di crisi non devono compromettere in alcun modo la protezione o la distruzione di materiale UE SEGRETISSIMO, ivi compresa l'attrezzatura di cifratura, il cui trattamento è prioritario rispetto a tutte le altre funzioni.

3. Le misure da adottare per la protezione e la distruzione dell'attrezzatura di cifratura in situazioni di emergenza sono contenute in istruzioni ad hoc.

4. Le istruzioni devono essere contenute in una busta sigillata ed essere disponibili in loco. Devono essere disponibili mezzi/strumenti per la distruzione.

23. MISURE DI SICUREZZA DA APPLICARE IN OCCASIONE DI RIUNIONI SPECIFICHE TENUTE FUORI DEI LOCALI DELLA COMMISSIONE E CONCERNENTI INFORMAZIONI CLASSIFICATE UE

23.1. Considerazioni generali

Quando riunioni della Commissione o altre riunioni importanti si tengono fuori dei locali della Commissione ed ove le particolari esigenze di sicurezza connesse con l'elevata sensibilità delle questioni o delle informazioni discusse lo giustifichino, sono adottate le misure di sicurezza descritte in appresso. Tali misure riguardano unicamente la protezione delle informazioni classificate UE: potrebbe essere necessario prevedere altre misure di sicurezza.

23.2. Responsabilità

23.2.1. *Il servizio di sicurezza della Commissione*

Il servizio di sicurezza della Commissione coopera con le autorità competenti dello Stato membro sul cui territorio si svolge la riunione (Stato membro ospitante) per garantire la sicurezza delle riunioni della Commissione o di altre riunioni importanti, nonché della sicurezza fisica dei principali delegati e del loro seguito. Per quanto riguarda la salvaguardia della sicurezza, esso provvede in particolare:

a) all'elaborazione di piani atti a contrastare le minacce alla sicurezza e far fronte agli incidenti connessi con la sicurezza, mediante misure intese in particolare a garantire che i documenti classificati UE siano custoditi negli uffici in condizioni di sicurezza;

b) all'adozione di misure intese a fornire una possibilità di accesso al sistema di comunicazioni della Commissione per la ricezione e la trasmissione di messaggi classificati UE. Lo Stato membro ospitante deve fornire inoltre, su richiesta, l'accesso a sistemi telefonici protetti.

Il servizio di sicurezza della Commissione funge da consulente in materia di sicurezza per la preparazione della riunione e invia in loco un suo rappresentante onde fornire, se necessario, assistenza e consulenza al responsabile della sicurezza della riunione (MSO) e alle delegazioni.

Ogni delegazione che prende parte ad una riunione deve designare un funzionario preposto alla sicurezza, incaricato di discutere con la rispettiva delegazione le questioni attinenti alla sicurezza e di mantenere i contatti con il responsabile della sicurezza della riunione e, se necessario, con il rappresentante del servizio di sicurezza della Commissione.

23.2.2. *Responsabile della sicurezza della riunione (MSO)*

Dovrebbe essere designato un responsabile della sicurezza della riunione competente per la preparazione generale e il controllo delle misure generiche di sicurezza interna, nonché per il coordinamento con le altre autorità di sicurezza interessate. Le misure adottate dal responsabile della sicurezza sono, di norma, del seguente tipo:

a) misure di protezione presso la sede della riunione onde scongiurare incidenti che potrebbero compromettere la sicurezza delle informazioni classificate UE eventualmente utilizzate nel corso della riunione;

b) controllo del personale cui è consentito l'accesso alla sede della riunione, alle aree riservate alle delegazioni ed alle sale delle conferenze e controllo di tutte le apparecchiature;

c) costante coordinamento con le autorità competenti dello Stato membro ospitante e con il servizio di sicurezza della Commissione;

d) inserimento nel dossier della riunione di istruzioni relative alla sicurezza, tenendo in debito conto quanto prescritto dalle presenti norme di sicurezza, e qualsiasi altra istruzione relativa alla sicurezza ritenuta necessaria.

23.3. Misure di sicurezza

23.3.1. *Zone di sicurezza*

Sono istituite le seguenti zone di sicurezza:

a) una zona di sicurezza di categoria II, comprendente la sala di redazione, gli uffici della Commissione e le apparecchiature di riproduzione, nonché gli uffici delle delegazioni a seconda dei casi;

b) una zona di sicurezza di categoria I, costituita dalla sala della conferenza e dalle cabine degli interpreti e dei tecnici audio;

c) zone amministrative, comprendenti l'area stampa e le aree della sede della riunione utilizzate a fini amministrativi, di ristorazione e di alloggio, nonché la zona immediatamente adiacente al centro stampa ed alla sede della riunione.

23.3.2. *Lasciapassare*

Il responsabile della sicurezza della riunione rilascia appositi badge secondo le richieste delle delegazioni ed in base alle loro esigenze operando, se necessario, una distinzione per l'accesso alle diverse zone di sicurezza.

Le istruzioni di sicurezza relative alla riunione prevedono che all'interno della sede della riunione tutti gli interessati portino sempre in modo ben visibile i loro badge, affinché il personale addetto alla sicurezza possa provvedere ai necessari controlli.

Oltre che ai partecipanti forniti di badge, l'accesso alla sede della riunione è consentito al minor numero possibile di persone. Il responsabile della sicurezza della riunione consente alle delegazioni nazionali di ricevere visitatori nel corso della riunione solo dietro richiesta delle stesse delegazioni. Ai visitatori viene rilasciato un apposito badge, previa compilazione di un lasciapassare recante il nome del visitatore e della persona visitata. I visitatori sono sempre accompagnati da una guardia di sicurezza o dalla persona visitata. L'accompagnatore porta il lasciapassare del visitatore e lo riconsegna, assieme al badge del visitatore, al personale di sicurezza quando il visitatore lascia la sede della riunione.

23.3.3. *Controllo degli apparecchi fotografici e degli apparecchi di registrazione audiovisiva*

Nella zona di sicurezza di categoria I è vietato introdurre apparecchi fotografici e di registrazione, ad eccezione delle apparecchiature dei fotografi e dei tecnici audio debitamente autorizzati dal responsabile della sicurezza della riunione.

23.3.4. *Controllo di valigie, computer portatili e plichi*

I detentori di lasciapassare cui è consentito l'accesso ad una zona di sicurezza possono di norma introdurvi senza controlli le loro valigie ed i loro computer portatili (solo autoalimentati). I plichi per le delegazioni vengono loro consegnati dopo essere stati ispezionati dal funzionario della delegazione addetto alla sicurezza, controllati mediante apparecchiature speciali o aperti dal personale addetto alla sicurezza per verificarne il contenuto. Se il responsabile della sicurezza della riunione lo ritiene necessario, si possono prevedere misure più rigorose per il controllo di valigie e plichi.

23.3.5. *Sicurezza tecnica*

Un'apposita squadra può garantire la sicurezza tecnica della sala di riunione e provvedere inoltre alla sorveglianza elettronica durante la riunione.

23.3.6. *Documenti delle delegazioni*

Le delegazioni sono responsabili dei documenti classificati UE che portano con sé alle riunioni. Sono inoltre responsabili della verifica e della sicurezza di detti documenti durante la loro utilizzazione nei locali ad esse assegnati. Per il trasporto di documenti classificati nella e dalla sede della riunione può essere chiesto l'aiuto degli Stati membri ospitanti.

23.3.7. *Custodia dei documenti in luogo sicuro*

Se la Commissione o le delegazioni non sono in grado di custodire i loro documenti classificati secondo le norme approvate, possono affidarli in busta sigillata, dietro ricevuta, al responsabile della sicurezza della riunione, che li custodisce in conformità di dette norme.

23.3.8. *Ispezione degli uffici*

Il responsabile della sicurezza della riunione provvede a che gli uffici della Commissione e delle delegazioni siano ispezionati al termine di ogni giornata lavorativa per verificare che tutti i documenti classificati UE siano al sicuro. In caso contrario adotta i provvedimenti necessari.

23.3.9. *Eliminazione dei rifiuti classificati*

Tutti i rifiuti sono trattati come rifiuti classificati UE, per la cui eliminazione vengono forniti alla Commissione e alle delegazioni cestini o pacchi della spazzatura. Prima di lasciare i locali ad essi assegnati, la Commissione e le delegazioni portano i loro rifiuti al responsabile della sicurezza della riunione, che provvede alla loro distruzione secondo le disposizioni del caso.

Al termine della riunione tutti i documenti detenuti dalla Commissione e dalle delegazioni e divenuti superflui sono trattati alla stregua di rifiuti. Prima di revocare le misure di sicurezza adottate per la riunione, viene effettuata un'accurata ispezione dei locali assegnati alla Commissione ed alle delegazioni. I documenti per i quali era stata firmata una ricevuta sono distrutti, ove possibile, come prescritto alla sezione 22.5.

24. VIOLAZIONE DELLA SICUREZZA E MANOMISSIONE DI INFORMAZIONI CLASSIFICATE UE

24.1. **Definizioni**

Una violazione della sicurezza è la conseguenza di atti o omissioni contrari a una disposizione della Commissione in materia di sicurezza, che potrebbero mettere a repentaglio o compromettere informazioni classificate UE.

Le informazioni classificate UE sono compromesse quando esse, o parte di esse, giungono in possesso di persone non autorizzate, vale a dire sprovviste dell'appropriato nullaosta di sicurezza o che non abbiano la necessità di conoscerle, o quando è probabile che si sia verificata tale circostanza.

Le informazioni classificate UE possono essere compromesse per disattenzione o negligenza, a seguito di indiscrezioni o come conseguenza delle attività di servizi che prendono di mira l'UE o gli Stati membri, per quanto riguarda le loro informazioni ed attività classificate UE, ovvero di organizzazioni sovversive.

24.2. **Relazioni sulle violazioni della sicurezza**

Tutte le persone che trattano informazioni classificate UE devono ricevere informazioni dettagliate sulle loro responsabilità in questo ambito e devono riferire immediatamente qualsiasi violazione della sicurezza di cui vengano a conoscenza.

Ove il responsabile locale della sicurezza o il responsabile della sicurezza della riunione riscontri o sia informato di una violazione della sicurezza relativa ad informazioni classificate UE o della perdita o della scomparsa di materiale classificato UE, adotta tempestivamente provvedimenti miranti a:

a) conservare le prove;

b) accertare i fatti;

c) valutare e limitare per quanto possibile i danni;

d) impedire che i fatti si ripetano;

e) informare le autorità competenti delle conseguenze della violazione della sicurezza.

A tale scopo vengono fornite le seguenti informazioni:

i) descrizione delle informazioni in questione, loro classificazione, numero di riferimento e numero di esemplare, data, originatore, oggetto e finalità del documento;

ii) breve descrizione delle circostanze in cui si è verificata la violazione della sicurezza, con indicazione della data e del periodo nel quale le informazioni sono state soggette al rischio di manomissione;

iii) se l'originatore sia stato o meno informato.

Non appena informata di una possibile violazione della sicurezza, ciascuna autorità di sicurezza riferisce immediatamente i fatti al servizio di sicurezza della Commissione.

I casi riguardanti informazioni UE RISERVATO devono essere riferiti solo quando presentino aspetti inconsueti.

Il membro della Commissione responsabile per le questioni della sicurezza, informato di una violazione della sicurezza:

a) ne dà notifica all'autorità d'origine dell'informazione classificata in questione;

b) chiede alle autorità competenti in materia di sicurezza di avviare le indagini;

c) coordina le indagini qualora sia interessata più di un'autorità competente in materia di sicurezza;

d) fa stilare una relazione sulle circostanze della violazione, con l'indicazione della data o del periodo nel quale essa potrebbe essersi verificata ed è stata riscontrata, ed una descrizione particolareggiata del contenuto e del grado di classificazione del materiale implicato. La relazione prende in considerazione anche i danni arrecati agli interessi dell'UE o di uno o più Stati membri e le misure adottate per impedire che i fatti si ripetano.

L'autorità d'origine informa i destinatari ed impartisce le istruzioni del caso.

24.3. **Procedimenti giudiziari**

Chiunque sia responsabile della compromissione di informazioni classificate UE è passibile di sanzioni disciplinari in conformità delle norme e dei regolamenti pertinenti, in particolare del titolo VI dello statuto. Tali sanzioni non pregiudicano eventuali ulteriori procedimenti giudiziari.

25. PROTEZIONE DELLE INFORMAZIONI CLASSIFICATE UE TRATTATE IN SISTEMI INFORMATICI E SISTEMI DI COMUNICAZIONE

25.1. **Introduzione**

25.1.1. *Considerazioni generali*

La strategia e le prescrizioni in materia di sicurezza si applicano a tutti i sistemi e a tutte le reti di comunicazioni e di informazioni (in seguito denominati sistemi) che trattano informazioni classificate di grado UE RISERVATISSIMO o grado superiore. Esse sono applicate in complemento alla decisione C (95) 1510 def. della Commissione, del 23 novembre 1995, sulla protezione dei sistemi informatici.

I sistemi che trattano informazioni UE RISERVATO richiedono anche misure di sicurezza atte a proteggere la riservatezza delle informazioni. Tutti i sistemi richiedono misure di sicurezza atte a proteggere l'integrità e la disponibilità dei sistemi stessi e delle informazioni in essi contenute.

La politica applicata dalla Commissione in materia di sicurezza informatica è caratterizzata dai seguenti elementi:

— essa costituisce parte integrante della sicurezza in generale ed integra tutti gli elementi di sicurezza dell'informazione, sicurezza del personale e sicurezza materiale,

— le responsabilità sono ripartite tra i proprietari dei sistemi tecnici, i proprietari delle informazioni classificate UE archiviate o trattate in sistemi tecnici, gli specialisti nel campo della sicurezza informatica e gli utenti,

— vengono descritti i principi e i requisiti in materia di sicurezza di ciascun sistema TI,

— tali principi e requisiti sono approvati da un'autorità designata,

— si tiene conto delle minacce e vulnerabilità specifiche al settore informatico.

25.1.2. *Minacce ai sistemi e loro vulnerabilità*

Si intende per minaccia la possibilità di una compromissione accidentale o deliberata della sicurezza. Nel caso dei sistemi, ciò implica la perdita di una o più delle caratteristiche di riservatezza, integrità e disponibilità. La vulnerabilità può essere definita come insufficienza o mancanza di controlli che rende più agevole o consente l'attuazione di una minaccia contro un bene o un bersaglio specifico.

Le informazioni classificate UE e non classificate trattate dai sistemi in forma compressa ai fini della rapidità di reperimento, comunicazione e utilizzo sono soggette a molteplici rischi, fra cui l'accesso alle informazioni da parte di utenti non abilitati o, viceversa, l'impossibilità di accesso per gli utenti abilitati. Altri rischi sono costituiti dalla divulgazione non autorizzata e dalla contaminazione, modifica o soppressione delle informazioni. Le apparecchiature in questione, complesse ed a volte fragili, sono inoltre costose e spesso difficili da riparare o da sostituire in tempi brevi.

25.1.3. *Obiettivo principale delle misure di sicurezza*

Obiettivo principale delle misure di sicurezza previste nella presente sezione è offrire protezione contro la divulgazione non autorizzata di informazioni classificate UE (perdita di riservatezza) e contro la perdita di integrità e di disponibilità delle informazioni. Per conseguire l'adeguata protezione di sicurezza di un sistema che tratta informazioni classificate UE, l'ufficio di sicurezza della Commissione deve specificare le opportune norme di sicurezza convenzionale, unitamente alle pertinenti procedure e tecniche di sicurezza speciali, progettate appositamente per ciascun sistema.

25.1.4. *Dichiarazione relativa ai requisiti di sicurezza specifici del sistema (SSRS)*

Per tutti i sistemi che trattano informazioni classificate UE RISERVATISSIMO o di grado superiore, il proprietario dei sistemi tecnici (TSO, cfr. sezione 25.3.4) e il proprietario delle informazioni (cfr. sezione 25.3.5) sono invitati a rilasciare una dichiarazione relativa ai requisiti di sicurezza specifici del sistema (SSRS), avvalendosi, ove necessario, dell'apporto e dell'assistenza del gruppo di progetto e dell'ufficio di sicurezza della Commissione (in qualità di autorità INFOSEC - IA, cfr. sezione 25.3.3), e con l'approvazione dell'autorità di accreditamento in materia di sicurezza (SAA, cfr. sezione 25.3.2).

Una SSRS è anche richiesta qualora la disponibilità e l'integrità delle informazioni classificate UE RISERVATO o non classificate siano ritenute essenziali dalla SAA.

La SSRS è formulata nelle primissime fasi dell'avvio del progetto e viene sviluppata ed ampliata con l'evoluzione del progetto, svolgendo differenti funzioni nelle diverse fasi del ciclo di vita del progetto e del sistema.

25.1.5. *Funzionamento in condizioni di sicurezza*

Tutti i sistemi che trattano informazioni classificate UE RISERVATISSIMO o di grado superiore sono accreditati per funzionare in uno o, ove sia giustificato dai requisiti durante diversi periodi, più di uno dei seguenti modi di funzionamento in condizioni di sicurezza, o nel loro equivalente nazionale:

a) esclusivo;

b) predominante;

c) multilivello.

25.2. Definizioni

Per «accreditamento» si intende l'autorizzazione e l'approvazione di un sistema per trattare informazioni classificate UE nel suo ambiente operativo.

Nota:

Tale accreditamento deve essere effettuato dopo che tutte le pertinenti procedure di sicurezza sono state attuate e una volta raggiunto un sufficiente livello di protezione delle risorse del sistema. L'accreditamento avviene di norma sulla base della SSRS e include:

a) una dichiarazione relativa all'obiettivo dell'accreditamento per il sistema, in particolare su quali gradi di classificazione delle informazioni saranno trattati e su quali modi di funzionamento in condizioni di sicurezza sono proposti per il sistema o la rete;

b) un esame sulla gestione del rischio atto a identificare le minacce e le vulnerabilità nonché le misure per contrastarle;

c) le procedure operative di sicurezza (SecOP) con una descrizione dettagliata delle operazioni proposte (ad esempio modi, servizi da fornire) e comprendenti una descrizione delle caratteristiche di sicurezza del sistema su cui si basa l'accreditamento;

d) il piano per l'attuazione e la manutenzione delle caratteristiche di sicurezza;

e) il piano per il collaudo, la valutazione e la certificazione iniziali e successivi della sicurezza del sistema o della rete;

f) la certificazione, ove richiesta, unitamente ad altri elementi di accreditamento.

Per «responsabile della sicurezza informatica a livello centrale» (CISO) si intende il funzionario che, nell'ambito di un servizio informatico centrale, coordina e sorveglia le misure di sicurezza per i sistemi a organizzazione centralizzata.

Per «certificazione» si intende il rilascio di una dichiarazione ufficiale, sulla base di un esame indipendente concernente il modo in cui è stata eseguita una valutazione e i risultati che ha prodotto, che indica in quale misura un sistema soddisfa il requisito di sicurezza o un prodotto per la sicurezza informatica offre le presunte prestazioni predefinite in materia di sicurezza.

Per «sicurezza delle comunicazioni» (COMSEC) si intende l'applicazione di misure di sicurezza alle telecomunicazioni al fine di negare alle persone non autorizzate informazioni preziose desumibili dal possesso e dall'analisi di tali comunicazioni o di assicurare l'autenticità di tali telecomunicazioni.

Nota:

Tali misure includono la sicurezza della crittografia, della trasmissione e dell'emissione nonché la sicurezza delle procedure, dei materiali, del personale, del documento e del computer.

Per «sicurezza informatica» (COMPUSEC) si intende l'applicazione a un sistema informatico di caratteristiche di sicurezza per l'hardware, il firmware e il software atte a proteggere le informazioni contro la divulgazione non autorizzata, la manipolazione, la modifica/soppressione, o a impedire tali atti, o a impedire l'interruzione di servizio.

Per «prodotto per la sicurezza informatica» si intende un elemento generico per la sicurezza informatica, destinato ad essere incorporato in un sistema TI ai fini di potenziare, o di offrire, la riservatezza, l'integrità e la disponibilità delle informazioni trattate.

Per «funzionamento esclusivo in condizioni di sicurezza» si intende un modo di funzionamento in cui TUTTE le persone che hanno accesso al sistema sono in possesso di un nullaosta di sicurezza per il grado più elevato di classificazione delle informazioni trattate nel sistema e con necessità di sapere comune rispetto a TUTTE le informazioni trattate nel sistema.

Note:

(1) Il fatto che vi sia una necessità di sapere comune indica che le caratteristiche del computer non devono necessariamente offrire una separazione delle informazioni all'interno del sistema.

(2) Le altre caratteristiche di sicurezza (ad esempio relative al materiale, al personale o alle procedure) sono conformi ai requisiti per il grado più elevato di classificazione e per tutte le designazioni di categoria delle informazioni trattate nel sistema.

Per «valutazione» si intende l'esame tecnico dettagliato da parte di un'autorità competente, degli aspetti di sicurezza di un sistema e di un prodotto per la sicurezza della crittografia o del computer.

Note:

(1) La valutazione accerta la presenza della funzionalità di sicurezza richiesta e l'assenza di effetti secondari compromettenti derivanti da tale funzionalità e valuta l'inalterabilità di tale funzionalità.

(2) La valutazione determina se e quanto sono soddisfatti i requisiti di sicurezza di un sistema, o le presunte prestazioni di sicurezza di un prodotto per la sicurezza del computer, e stabilisce il livello di attendibilità del sistema o della funzione di fiducia del prodotto per la sicurezza del computer o della crittografia.

Per «proprietario delle informazioni» (IO) si intende l'autorità (capo servizio) responsabile della creazione, del trattamento e dell'utilizzazione delle informazioni, inclusa la facoltà di decidere chi può avere accesso a queste ultime.

Per «sicurezza dell'informazione» (INFOSEC) si intende l'applicazione di misure di sicurezza atte a proteggere le informazioni elaborate, archiviate o trasmesse da sistemi di comunicazione, di informazione o da altri sistemi elettronici contro la perdita di riservatezza, integrità o disponibilità, accidentale o intenzionale, nonché a impedire la perdita di integrità e di disponibilità dei sistemi stessi.

Le misure INFOSEC comprendono la sicurezza del computer, della trasmissione, dell'emissione e della crittografia nonché l'individuazione, la documentazione e la neutralizzazione di minacce nei confronti dell'informazione e dei sistemi.

Per «area TI» si intende un'area che contiene uno o più computer, le loro locali periferiche e unità di archiviazione, le unità di controllo e l'attrezzatura specializzate per le reti e le comunicazioni.

Nota:

La definizione non include un'area separata in cui sono situati i dispositivi periferici o i terminali/postazioni remoti anche qualora detti dispositivi siano connessi all'attrezzatura collocata nell'area TI.

Per «rete TI» si intende l'organizzazione, geograficamente diffusa, di sistemi TI interconnessi per lo scambio di dati, comprendente i componenti dei sistemi TI interconnessi e la loro interfaccia con le reti dati o le reti di comunicazione di sostegno.

Note:

(1) Una rete TI può usare i servizi di una o più reti di comunicazione interconnesse per lo scambio di dati: varie reti TI possono usare i servizi di una rete di comunicazioni comune.

(2) Una rete TI è denominata «locale» se collega vari computer nel medesimo sito.

Le «caratteristiche di sicurezza di una rete TI» includono le caratteristiche di sicurezza del sistema TI dei singoli sistemi che compongono la rete unitamente ai componenti e agli elementi aggiuntivi associati con la rete in quanto tale (per esempio le comunicazioni di rete, i meccanismi e le procedure per l'identificazione e l'etichettatura di sicurezza, i controlli di accesso, i programmi e gli audit trail) necessari per fornire un livello di protezione accettabile delle informazioni classificate.

Per «sistema TI» si intende un insieme di attrezzature, metodi e procedure e, se necessario, di personale, organizzato in modo da compiere funzioni di trattamento delle informazioni.

Note:

(1) Si tratta di un insieme di strutture, configurate per trattare informazioni all'interno del sistema

(2) Tali sistemi possono essere a sostegno di applicazioni di consultazione, comando, controllo e comunicazione, di applicazioni scientifiche o amministrative, incluso il trattamento testi.

(3) Un sistema è generalmente definito in base agli elementi posti sotto il controllo di un unico TSO.

(4) Un sistema TI può contenere sottosistemi alcuni dei quali sono essi stessi sistemi TI.

Le «caratteristiche di sicurezza di un sistema TI» comprendono tutte le funzioni e le caratteristiche hardware/firmware/software, le procedure operative, le procedure di responsabilità, i controlli di accesso, l'area TI, l'area di terminali/postazioni remoti, i vincoli della gestione, la struttura e i dispositivi materiali, i controlli del personale e delle comunicazioni necessari per fornire un livello accettabile di protezione delle informazioni classificate da trattare nel sistema TI.

Per «responsabile della sicurezza informatica a livello locale» (LISO) si intende il funzionario che, nell'ambito di un servizio della Commissione, coordina e sorveglia le misure di sicurezza relative al settore di sua competenza.

Per «funzionamento multilivello in condizioni di sicurezza» si intende un modo di funzionamento in cui NON TUTTE le persone che hanno accesso al sistema sono in possesso di un nullaosta di sicurezza al grado più elevato di classificazione delle informazioni trattate nel sistema, e NON TUTTE le persone con accesso al sistema hanno una necessità di sapere comune rispetto alle informazioni trattate nel sistema.

Note:

(1) Questo modo di funzionamento consente attualmente il trattamento di informazioni di diversi gradi di classificazione e con diverse designazioni di categoria.

(2) Il fatto che non tutte le persone siano in possesso di un nullaosta di sicurezza del grado più elevato, associato ad una mancanza di necessità di sapere comune, indica che le caratteristiche di sicurezza del computer devono offrire un accesso selettivo alle informazioni nel sistema e la loro separazione.

Per «area di terminali/postazioni remoti» si intende un'area contenente alcune attrezzature informatiche, i suoi dispositivi locali periferici o terminali/postazioni e qualsiasi attrezzatura di comunicazione associata, separata dall'area TI.

Per «procedure operative di sicurezza» si intendono le procedure elaborate dal proprietario dei sistemi tecnici che definiscono i principi da adottare in materia di sicurezza, le procedure operative da seguire e le responsabilità del personale.

Per «funzionamento predominante in condizioni di sicurezza» si intende un modo di funzionamento in cui TUTTE le persone che hanno accesso al sistema sono in possesso di un nullaosta di sicurezza al grado più elevato di classificazione delle informazioni trattate nel sistema, ma NON TUTTE le persone con accesso al sistema hanno una necessità di sapere comune rispetto alle informazioni trattate nel sistema.

Note:

(1) La mancanza di una necessità di sapere comune indica che le caratteristiche di sicurezza del computer devono offrire un accesso selettivo alle informazioni nel sistema e la separazione delle medesime.

(2) Le altre caratteristiche di sicurezza (ad esempio relative al materiale, al personale o alle procedure) sono conformi ai requisiti per il grado più elevato di classificazione e per tutte le designazioni di categoria delle informazioni trattate nel sistema.

(3) Tutte le informazioni trattate o messe a disposizione nel sistema in base a questo modo di funzionamento, unitamente all'output che ne deriva, sono protette come se rientrassero potenzialmente nella designazione di categoria e nel grado più elevato di classificazione delle informazioni trattate fino a prova contraria, a meno che sussista un livello di fiducia accettabile nei confronti della funzione di etichettatura già presente.

La «dichiarazione relativa ai requisiti di sicurezza specifici del sistema» (SSRS) è una dichiarazione completa ed esplicita relativa ai principi di sicurezza da osservare e ai requisiti particolareggiati di sicurezza da rispettare. È basata sulla politica della Commissione in materia di sicurezza e di valutazione del rischio, oppure imposta da parametri che disciplinano l'ambiente operativo, il grado più basso di nullaosta di sicurezza del personale, il grado più alto di classificazione delle informazioni trattate, il modo di funzionamento in condizioni di sicurezza o le esigenze degli utenti. La SSRS forma parte integrante della documentazione sul progetto sottoposta alle pertinenti autorità ai fini dell'approvazione tecnica, finanziaria e di sicurezza. Nella sua forma definitiva, la SSRS costituisce un elenco completo di quanto è necessario per garantire la sicurezza del sistema.

Per «proprietario dei sistemi tecnici» (TSO) si intende l'autorità responsabile della creazione, della manutenzione, del funzionamento e della chiusura di un sistema.

Per «contromisure dell'effetto tempesta» si intendono misure di sicurezza destinate a proteggere l'attrezzatura e le infrastrutture di comunicazione contro il rischio di compromissione delle informazioni classificate dovuta a emissioni elettromagnetiche non intenzionali e alla conduttività.

25.3. **Responsabilità in materia di sicurezza**

25.3.1. *Considerazioni generali*

Tra le responsabilità consultive del gruppo consultivo della Commissione per le politiche della sicurezza, di cui alla sezione 12, rientrano le questioni inerenti all'INFOSEC. Il suddetto gruppo organizza le proprie attività in modo da fornire una consulenza qualificata in materia.

Spetta all'ufficio di sicurezza della Commissione emanare disposizioni INFOSEC dettagliate, sulla base di quanto disposto al presente capitolo.

In caso di problemi concernenti la sicurezza (incidenti, violazioni, ecc.) l'ufficio di sicurezza della Commissione prende misure immediate.

L'ufficio di sicurezza della Commissione dispone di un'unità INFOSEC.

25.3.2. *L'autorità di accreditamento in materia di sicurezza (SAA)*

Il capo dell'ufficio di sicurezza della Commissione è l'autorità di accreditamento in materia di sicurezza (SAA) per la Commissione. La SAA è responsabile nell'ambito generale della sicurezza e negli ambiti specifici dell'INFOSEC (sicurezza delle comunicazioni, sicurezza Crypto e sicurezza Tempest).

La SAA è responsabile di accertare la conformità dei sistemi con la politica della Commissione in materia di sicurezza. Tra i suoi compiti rientra il rilascio dell'approvazione di un sistema per il trattamento delle informazioni classificate UE ad un determinato grado di classificazione nel suo ambiente operativo.

La competenza della SAA della Commissione si estende a tutti i sistemi in funzione all'interno dei locali della Commissione. Quando diversi componenti di un sistema rientrano nella competenza della SAA della Commissione e di altre SAA, tutte le parti interessate nominano un comitato comune di accreditamento posto sotto il coordinamento della SAA della Commissione.

25.3.3. *L'autorità INFOSEC (IA)*

Il capo dell'unità INFOSEC dell'ufficio di sicurezza della Commissione è l'autorità INFOSEC per la Commissione. L'autorità INFOSEC è responsabile delle seguenti attività:

— fornire consulenza e assistenza tecnica alla SAA,
— assistere lo sviluppo della SSRS,
— riesaminare la SSRS per accertarne la coerenza con le presenti norme di sicurezza e i documenti relativi alla politica e all'architettura INFOSEC,
— partecipare alle commissioni/ai comitati di accreditamento ove necessario nonché fornire alla SAA raccomandazioni INFOSEC sull'accreditamento,
— fornire supporto alle attività di formazione e di informazione INFOSEC,
— fornire consulenza tecnica nelle indagini sugli incidenti connessi con l'INFOSEC,
— definire orientamenti tecnici strategici onde garantire che sia utilizzato unicamente software autorizzato.

25.3.4. *Il proprietario dei sistemi tecnici (TSO)*

La responsabilità dell'attuazione dei controlli e del funzionamento dei dispositivi di sicurezza di un sistema spetta al proprietario di quel sistema, il «proprietario dei sistemi tecnici» (TSO). Per i sistemi gestiti a livello centrale è nominato un «responsabile della sicurezza informatica a livello centrale» (CISO). Ciascun servizio nomina, se necessario, un «responsabile della sicurezza informatica a livello locale» (LISO). Le responsabilità di un TSO includono la creazione delle «procedure operative di sicurezza» (SecOP) e permangono lungo tutto il ciclo di vita di un sistema, dalla fase di concezione del progetto alla sua disattivazione finale.

Il TSO specifica le norme e le procedure di sicurezza che il fornitore del sistema è tenuto a rispettare.

Se necessario, il TSO può delegare una parte delle sue responsabilità a un responsabile della sicurezza informatica a livello locale. Le varie mansioni INFOSEC possono essere svolte da una sola persona.

25.3.5. Il *proprietario delle informazioni (IO)*

Il proprietario delle informazioni (IO) è responsabile delle informazioni classificate UE (e delle altre informazioni) che devono essere introdotte, elaborate e prodotte in sistemi tecnici. Egli definisce i requisiti relativi all'accesso a tali informazioni nei sistemi. Questa responsabilità può essere delegata a un gestore delle informazioni o a un gestore di basi di dati nel settore di sua competenza.

25.3.6. *Utenti*

Tutti gli utenti sono tenuti a garantire che le loro azioni non compromettano la sicurezza del sistema che utilizzano.

25.3.7. *Formazione INFOSEC*

La formazione e l'informazione INFOSEC è disponibile per tutto il personale che ne ha bisogno.

25.4. **Misure di sicurezza non tecniche**

25.4.1. *Sicurezza del personale*

Gli utenti del sistema devono essere in possesso di nulla osta di sicurezza ed avere necessità di sapere, in funzione della classificazione e del contenuto delle informazioni trattate dal loro specifico sistema. L'accesso a determinate attrezzature o a informazioni inerenti alla sicurezza dei sistemi richiede uno speciale nulla osta di sicurezza rilasciato in base alle procedure della Commissione.

La SAA designa tutti i posti sensibili e specifica il grado del nulla osta e la sorveglianza necessaria da parte delle persone che li ricoprono.

I sistemi sono specificati e progettati in modo da facilitare l'attribuzione dei compiti e delle responsabilità al personale onde evitare che una sola persona abbia la conoscenza o il controllo totali dei punti nevralgici per la sicurezza del sistema.

Le aree TI e quelle di terminali/postazioni remoti in cui la sicurezza del sistema può essere modificata non sono occupate da un solo funzionario/altro dipendente abilitato.

I dispositivi di sicurezza di un sistema possono essere modificati solo da almeno due persone autorizzate che operano congiuntamente.

25.4.2. *Sicurezza materiale*

Le aree TI e le aree di terminali/postazioni remoti (quali definite nella sezione 25.2) in cui sono trattate informazioni classificate UE RISERVATISSIMO o di grado superiore con strumenti TI, o in cui è possibile un accesso a tali informazioni, sono classificate secondo il caso come aree di sicurezza di categoria UE I o II.

25.4.3. *Controllo dell'accesso a un sistema*

Tutte le informazioni e il materiale che consentono il controllo dell'accesso a un sistema sono protette da disposizioni commisurate al grado di classificazione e alla designazione di categoria più elevati delle informazioni cui danno accesso.

Le informazioni e il materiale per il controllo dell'accesso che non sono più utilizzati a questo scopo vengono distrutte conformemente alla sezione 25.5.4.

25.5. **Misure tecniche di sicurezza**

25.5.1. *Sicurezza delle informazioni*

L'originatore delle informazioni è tenuto a identificare e classificare tutti i documenti contenenti informazioni, siano essi su supporto cartaceo o informatico. Ciascuna pagina delle copie cartacee viene contrassegnata, in testa e in calce, con la pertinente classificazione. I documenti, che siano su supporto cartaceo o informatico, hanno la classificazione più elevata tra quelle attribuite all'informazione utilizzata per produrli. Il modo di funzionamento di un sistema può anche avere un impatto sulla classificazione dei documenti prodotti da tale sistema.

I servizi della Commissione e coloro che, al loro interno, sono in possesso di informazioni sono tenuti a valutare i problemi inerenti al raggruppamento di singoli elementi informativi, e alle deduzioni che si possono trarre dagli elementi connessi, nonché a determinare se una classificazione di grado più elevato sia pertinente per la totalità delle informazioni così raggruppate.

Il fatto che l'informazione possa essere formulata come un codice abbreviato, un codice di trasmissione o qualsiasi altra forma di rappresentazione binaria non conferisce alcuna protezione della sicurezza e non deve, pertanto, incidere sulla classificazione dell'informazione.

Quando l'informazione è trasferita da un sistema ad un altro, l'informazione è protetta durante il trasferimento e nel sistema ricevente in modo commisurato alla classificazione e alla categoria originarie dell'informazione.

Tutti i mezzi di archiviazione informatica sono trattati in modo commisurato alla classificazione più elevata dell'informazione archiviata o del contrassegno apposto sul mezzo, e opportunamente protetti in ogni momento.

I mezzi di archiviazione informatica riutilizzabili usati per registrare informazioni classificate UE mantengono la classificazione più elevata per la quale sono stati usati finché le informazioni in questione non vengono declassate o declassificate e il mezzo di archiviazione riclassificato di conseguenza, oppure il mezzo declassificato o distrutto con una procedura approvata dalla SAA (cfr. sezione 25.5.4).

25.5.2. *Controllo e responsabilità delle informazioni*

I log automatici (audit trail) o manuali sono tenuti quale traccia dell'accesso alle informazioni classificate UE SEGRETO o di grado superiore. Queste tracce sono conservate conformemente alle presenti norme di sicurezza.

I prodotti classificati UE detenuti nella zona TI possono essere trattati come un elemento classificato e non necessitano di registrazione, purché il materiale sia identificato, contrassegnato con la sua classificazione e controllato in modo appropriato.

Allorché un sistema che tratta informazioni classificate UE genera dati che vengono trasmessi da un'area TI all'area di terminali/postazioni remoti, vengono istituite procedure, approvate dalla SAA, per controllare e registrare i dati trasmessi. Per le classificazioni di grado UE SEGRETO o superiore tali procedure includono specifiche istruzioni per la responsabilità delle informazioni.

25.5.3. *Trattamento e controllo dei supporti informatici rimovibili*

Tutti i supporti informatici rimovibili classificati UE RISERVATISSIMO o di grado superiore sono trattati come materiale classificato cui si applicano le norme generali. I contrassegni di identificazione e classificazione devono essere adattati alle specifiche caratteristiche fisiche dei supporti, in modo da renderli chiaramente riconoscibili.

Spetta agli utenti assicurare che le informazioni classificate UE siano archiviate su supporti provvisti dell'appropriato contrassegno di classificazione e adeguatamente protetti. Sono stabilite procedure atte ad assicurare che, per tutti i gradi di classificazione UE, l'archiviazione delle informazioni su supporti informatici avvenga in conformità delle presenti norme di sicurezza.

25.5.4. *Declassificazione e distruzione di supporti informatici*

I supporti informatici utilizzati per la registrazione di informazioni classificate UE possono essere declassati o declassificati a condizione che siano applicate procedure approvate dalla SAA.

I supporti informatici che hanno contenuto informazioni UE SEGRETISSIMO o informazioni di una categoria speciale non sono declassificati né riutilizzati.

I supporti informatici che non possono essere declassificati o riutilizzati sono distrutti secondo una procedura approvata dalla SAA.

25.5.5. *Sicurezza delle comunicazioni*

Il capo dell'ufficio di sicurezza della Commissione è l'autorità Crypto.

Quando informazioni classificate UE sono trasmesse per via elettromagnetica, si applicano misure speciali atte a proteggere la riservatezza, l'integrità e la disponibilità della trasmissione. La SAA stabilisce i requisiti relativi alla protezione delle trasmissioni dalla detezione e dalle intercettazioni. Le informazioni trasmesse all'interno di un sistema di comunicazioni sono protette tenendo conto dei requisiti di riservatezza, integrità e disponibilità.

I metodi crittografici, e i prodotti connessi, che si rendano necessari per la protezione della riservatezza, dell'integrità e della disponibilità sono specificamente approvati a tal fine dalla SAA in qualità di autorità Crypto.

Durante la trasmissione, la riservatezza delle informazioni classificate UE SEGRETO o di grado superiore è protetta mediante metodi o prodotti crittografici approvati dal membro della Commissione responsabile per le questioni della sicurezza previa consultazione del gruppo consultivo della Commissione per le politiche della sicurezza. Durante la trasmissione, la riservatezza delle informazioni classificate UE RISERVATISSIMO o UE RISERVATO è protetta mediante metodi o prodotti crittografici approvati dall'autorità Crypto della Commissione previa consultazione del gruppo consultivo della Commissione per le politiche della sicurezza.

Specifiche istruzioni di sicurezza approvate dall'ufficio di sicurezza della Commissione previa consultazione del gruppo consultivo della Commissione per le politiche della sicurezza contengono norme particolareggiate applicabili alla trasmissione di informazioni classificate UE.

In circostanze operative eccezionali le informazioni classificate UE RISERVATO, UE RISERVATISSIMO e UE SEGRETO possono essere trasmesse sotto forma di testo in chiaro, previa esplicita autorizzazione per ogni singolo caso e opportuna registrazione ad opera del proprietario delle informazioni. Le circostanze eccezionali di cui sopra si verificano:

a) in situazioni di crisi, conflitti o guerre imminenti o già in corso e

b) quando la rapidità di consegna è della massima importanza e non sono disponibili strumenti di cifratura, nonché quando si ritiene che le informazioni trasmesse non possano essere sfruttate con rapidità tale da influire negativamente sulle operazioni.

Un sistema deve essere in grado di negare con certezza ad una o tutte le sue postazioni o ai suoi terminali remoti l'accesso ad informazioni classificate UE, se necessario disconnettendoli materialmente o mediante speciali caratteristiche del software approvate dalla SAA.

25.5.6. *Misure di sicurezza concernenti l'installazione e le radiazioni*

Le specifiche relative all'installazione iniziale dei sistemi e a qualsiasi successiva modifica di rilievo prevedono che l'installazione sia effettuata da installatori provvisti di nulla osta di sicurezza sotto la costante sorveglianza di personale tecnico qualificato abilitato all'accesso ad informazioni aventi un grado di classificazione UE equivalente al grado più alto delle informazioni che il sistema dovrà archiviare o trattare.

I sistemi che trattano informazioni classificate UE RISERVATISSIMO o di grado superiore sono protetti in modo tale che la loro sicurezza non possa essere minacciata da radiazioni o da una conduttività compromettenti, il cui studio e la cui prevenzione sono designati dal termine «TEMPEST».

Le contromisure dell'«effetto tempesta» sono esaminate e approvate dall'autorità Tempest (cfr. sezione 25.3.2).

25.6. **Sicurezza durante il trattamento**

25.6.1. *Procedure operative di sicurezza (SecOP)*

Le procedure operative di sicurezza (SecOP) definiscono i principi da adottare in materia di sicurezza, le procedure operative da seguire e le responsabilità del personale. Le SecOP sono elaborate sotto la responsabilità del proprietario dei sistemi tecnici (TSO).

25.6.2. *Protezione del software/gestione della configurazione*

Il livello di protezione dei programmi applicativi è determinato in base ad una valutazione della classificazione di sicurezza dei programmi stessi piuttosto che delle informazioni che devono trattare. Le versioni dei software in uso devono essere verificate ad intervalli regolari per assicurarne l'integrità ed il corretto funzionamento.

Versioni nuove o modificate dei software vengono utilizzate per il trattamento di informazioni classificate UE solo dopo essere state verificate dal TSO.

25.6.3. *Controlli contro la presenza di software «maligni»/virus informatici*

Controlli contro la presenza di software «maligni»/virus informatici sono effettuati periodicamente secondo quanto prescritto dalla SAA.

Prima di essere immessi in un sistema, tutti i supporti informatici introdotti nella Commissione devono essere controllati al fine di rilevare l'eventuale presenza di software «maligni» o virus informatici.

25.6.4. *Manutenzione*

Nei contratti e nelle procedure concernenti la manutenzione periodica e su richiesta dei sistemi per cui sia stata stilata una SSRS sono specificati i requisiti e le disposizioni applicabili al personale addetto alla manutenzione ed alle relative apparecchiature che entrano in una zona TI.

Tali requisiti e tali procedure sono chiaramente indicati, rispettivamente, nella SSRS e nelle SecOP. Le operazioni di manutenzione di competenza del contraente che richiedono procedure di telediagnostica sono consentite solo in circostanze eccezionali, sotto rigoroso controllo ed esclusivamente previa approvazione della SAA.

25.7. **Fornitura**

25.7.1. *Considerazioni generali*

Qualsiasi prodotto relativo alla sicurezza da utilizzare con il sistema oggetto della fornitura, deve già essere stato valutato e certificato oppure essere in fase di valutazione e certificazione da parte di un apposito organismo di uno degli Stati membri dell'UE, secondo criteri riconosciuti a livello internazionale (quali i criteri comuni per la valutazione della sicurezza delle tecnologie dell'informazione: cfr. ISO 15408). Procedure specifiche sono richieste per ottenere l'approvazione della CCAC.

Per decidere se noleggiare piuttosto che acquistare un'attrezzatura, specie supporti informatici, occorre tener presente che, una volta utilizzata per le informazioni classificate UE, tale attrezzatura non potrà essere resa disponibile al di fuori di un ambiente adeguatamente protetto senza prima essere declassificata con il consenso della SAA e che non sempre detto consenso sarà possibile.

25.7.2. *Accreditamento*

Tutti i sistemi che necessitano in via preventiva, per il trattamento di informazioni classificate UE, di una dichiarazione relativa ai requisiti di sicurezza specifici del sistema sono accreditati dalla SAA sulla scorta delle informazioni fornite nella suddetta dichiarazione, delle SecOP e di qualsiasi altra documentazione pertinente. I sottosistemi e i terminali/postazioni remoti sono accreditati in quanto parte di tutti i sistemi a cui sono collegati. Quando un sistema serve sia la Commissione che altre organizzazioni, la Commissione e le competenti autorità incaricate della sicurezza approvano l'accreditamento di comune accordo.

Il processo di accreditamento può essere espletato secondo un'apposita strategia adeguata ad un determinato sistema, definita dalla SAA.

25.7.3. *Valutazione e certificazione*

Prima di essere accreditati, in taluni casi, gli elementi di sicurezza di un sistema nel suo insieme — hardware, firmware e software — sono valutati e certificati idonei alla salvaguardia delle informazioni al grado di classificazione desiderato.

I requisiti per la valutazione e certificazione sono inclusi nella progettazione del sistema e chiaramente definiti nella SSRS.

I processi di valutazione e certificazione sono espletati secondo linee direttrici approvate da personale tecnicamente qualificato e adeguatamente abilitato che opera a nome del TSO.

I gruppi a ciò preposti possono essere inviati da un'autorità nazionale di valutazione o certificazione designata oppure da suoi rappresentanti designati, ad esempio un appaltatore competente e abilitato.

I processi di valutazione e certificazione richiesti possono essere di livello inferiore (ed includere, ad esempio, solo gli aspetti dell'integrazione) qualora i sistemi siano basati su prodotti per la sicurezza dei computer valutati e certificati in ambito nazionale.

25.7.4. *Verifica sistematica degli elementi di sicurezza per la proroga dell'accreditamento*

Il TSO stabilisce procedure di controllo sistematico atte a garantire che tutti gli elementi di sicurezza del sistema siano ancora efficaci.

I tipi di cambiamenti che renderebbero necessario un riaccreditamento o che richiedono l'approvazione preventiva della SAA sono chiaramente individuati ed enunciati nella SSRS. Dopo qualsiasi modifica, riparazione o disfunzione che possa avere ripercussioni sugli elementi di sicurezza del sistema, il TSO provvede a far effettuare una verifica per assicurare il corretto funzionamento dei suddetti elementi. La proroga dell'accreditamento del sistema dipende normalmente da un risultato soddisfacente delle verifiche.

Tutti i sistemi dotati di elementi di sicurezza sono periodicamente ispezionati o riesaminati dalla SAA. Per i sistemi che trattano informazioni classificate UE SEGRETISSIMO, le ispezioni hanno luogo almeno una volta l'anno.

25.8. Utilizzo temporaneo o occasionale

25.8.1. Sicurezza dei microcomputer/personal computer

I microcomputer/personal computer (PC) muniti di disco fisso (o altri mezzi di archiviazione permanente), funzionanti sia autonomamente sia in rete, e i dispositivi informatici portatili (quali PC portatili e notebook elettronici) provvisti di disco rigido fisso sono considerati mezzi di archiviazione delle informazioni alla stessa stregua dei dischetti o altri supporti informatici rimovibili.

A tali attrezzature è attribuito il livello di protezione, in termini di accesso, gestione, archiviazione e trasporto, corrispondente al più alto grado di classificazione delle informazioni archiviate o elaborate (finché passeranno poi ad un livello di protezione inferiore o subiranno una declassificazione conformemente a procedure approvate).

25.8.2. Uso di attrezzatura informatica privata per i lavori ufficiali della Commissione

Per il trattamento delle informazioni classificate UE è vietato utilizzare supporti informatici, software e hardware (quale PC e dispositivi informatici portatili) che siano dotati di memoria, di proprietà privata e rimovibili.

Hardware, software e supporti vari di proprietà privata non possono essere introdotti in nessuna zona di categoria I o II dove sono trattate informazioni classificate UE senza l'autorizzazione scritta del capo dell'ufficio di sicurezza della Commissione. Tale autorizzazione può essere concessa solo in casi eccezionali per motivi tecnici.

25.8.3. Uso di attrezzatura informatica appartenente a un appaltatore o fornita dagli Stati membri per i lavori ufficiali della Commissione

Il capo dell'ufficio di sicurezza della Commissione può permettere l'utilizzo di attrezzatura IT e software detenuti da un appaltatore per i lavori ufficiali della Commissione. Può essere altresì autorizzato l'utilizzo di attrezzatura e software forniti dagli Stati membri: in tal caso, detta attrezzatura è posta sotto controllo e iscritta nell'apposito inventario della Commissione. Nell'uno o nell'altro caso, se l'attrezzatura serve al trattamento di informazioni classificate UE, si consulta la SAA competente ai fini di un'adeguata presa in considerazione e applicazione degli elementi INFOSEC applicabili al suo utilizzo.

26. COMUNICAZIONE DI INFORMAZIONI CLASSIFICATE UE A STATI TERZI O ORGANIZZAZIONI INTERNAZIONALI

26.1.1. Principi che regolano la comunicazione di informazioni classificate UE

La comunicazione di informazioni classificate UE a Stati terzi o organizzazioni internazionali è decisa collegialmente dalla Commissione in base:

— alla natura e al contenuto delle informazioni stesse,

— alla necessità di sapere dei destinatari,

— all'entità dei vantaggi per l'UE.

All'originatore dell'informazione classificata UE è chiesto il consenso alla comunicazione.

Siffatte decisioni sono prese caso per caso, a seconda:

— del livello di cooperazione auspicato con gli Stati terzi o le organizzazioni internazionali interessati,

— della loro affidabilità — dipendente dal livello di sicurezza che sarebbe attribuito alle informazioni classificate UE affidate a detti Stati o organizzazioni nonché dalla conformità delle norme di sicurezza ivi applicabili a quelle applicate nell'UE; a tal riguardo la Commissione si avvale del parere tecnico del gruppo consultivo della Commissione per le politiche della sicurezza.

L'accettazione di informazioni classificate UE da parte di Stati terzi o organizzazioni internazionali implica la garanzia che saranno utilizzate esclusivamente agli scopi per cui sono state comunicate o scambiate e che sarà loro assicurata la protezione richiesta dalla Commissione.

26.1.2. Livelli

Una volta decisa la comunicazione o lo scambio di informazioni classificate con un determinato Stato o organizzazione internazionale, la Commissione decide il livello di cooperazione possibile, che dipenderà soprattutto dalla politica seguita in materia di sicurezza e dalla normativa applicata da tale Stato o organizzazione.

I livelli di cooperazione sono tre:

Primo livello

Cooperazione con Stati terzi o organizzazioni internazionali la cui politica e normativa in materia di sicurezza sono molto affini a quelle dell'UE.

Secondo livello

Cooperazione con Stati terzi o organizzazioni internazionali la cui politica e normativa in materia di sicurezza sono notevolmente diverse da quelle dell'UE.

Terzo livello

Cooperazione di carattere occasionale con Stati terzi o organizzazioni internazionali di cui non si possono valutare la politica e la normativa in materia di sicurezza.

Il livello di cooperazione determina le procedure e le norme di sicurezza da seguire, descritte dettagliatamente nelle appendici 3, 4 e 5.

26.1.3. *Accordi in materia di sicurezza*

Constatata la necessità permanente o a lungo termine di uno scambio di informazioni classificate tra la Commissione e Stati terzi o altre organizzazioni internazionali, la Commissione procede alla stesura di «accordi sulle procedure di sicurezza per lo scambio di informazioni classificate» con essi, dove sono definite le finalità della cooperazione e le disposizioni reciproche sulla protezione delle informazioni scambiate.

Nel caso di una cooperazione occasionale di terzo livello, per definizione limitata nel tempo e nelle finalità, un semplice memorandum d'intesa in cui siano definiti la natura delle informazioni classificate da scambiare e gli obblighi reciproci ad esse relativi può sostituirsi agli «accordi sulle procedure di sicurezza per lo scambio di informazioni classificate» purché il grado di classificazione non sia più elevato di UE RISERVATO.

Prima di essere presentati alla Commissione per una decisione, i progetti di accordi sulle procedure di sicurezza o di memorandum d'intesa sono approvati dal gruppo consultivo della Commissione per le politiche della sicurezza.

Le NSA degli Stati membri forniscono al membro della Commissione responsabile per le questioni della sicurezza tutta l'assistenza necessaria a garantire che le informazioni da divulgare siano utilizzate e protette conformemente ai suddetti accordi sulle procedure di sicurezza o ai memorandum d'intesa.

Appendice 1

RAFFRONTO TRA LE CLASSIFICAZIONI NAZIONALI DI SICUREZZA

Classificazione UE	UE SEGRETISSIMO	UE SEGRETO	UE RISERVATISSIMO	UE RISERVATO
Classificazione NATO (1)				
Classificazione UEO	FOCAL SEGRETISSIMO	UEO SEGRETO	UEO RISERVATISSIMO	UEO RISERVATISSIMO
Classificazione EURATOM (2)	EURA Strettamente SEGRETO	EURA Segreto	EURA Confidenziale	EURA Diffusione riservata
Belgio	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Danimarca	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germania	STRENG GEHEIM	GEHEIM	VS (3) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Grecia	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Spagna	Secreto	Reservado	Confidencial	Difusion Limitada
Francia	Très Secret Défense (4)	Secret Défense	Confidentiel Défense	Diffusion restreinte
Irlanda	Top Secret	Secret	Confidential	Restricted
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Lussemburgo	Très Secret	Secret	Confidentiel	Diffusion restreinte
Paesi bassi	Stg. Zeer Geheim	Stg. Geheim	Stg. Confidentieel	
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Portogallo	Muito Secreto	Secreto	Confidencial	Reservado
Finlandia	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Svezia	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Regno Unito	Top Secret	Secret	Confidential	Restricted

(1) NATO — la corrispondenza con i livelli di classificazione nato sarà definita una volta negoziato l'accordo in materia di sicurezza tra la Commissione e la NATO.
(2) Regolamento (EURATOM) n. 3, del 31 luglio 1958, relativo alla protezione delle informazioni classificate («cognizioni segrete») dell'EURATOM.
(3) Germania: VS = Verschlusssache.
(4) Francia: la classificazione «Très Secret Défense», che riguarda questioni prioritarie per il governo, può essere modificata solo con l'autorizzazione del Primo ministro.

Appendice 2

GUIDA PRATICA ALLA CLASSIFICAZIONE

La presente guida è uno strumento indicativo, che non può essere interpretato come variante delle disposizioni sostanziali di cui alle sezioni 16, 17, 20 e 21.

Classificazione	Quando	Chi	Apposizione delle classificazioni	Declassamento/declassificazione/distruzione	
				Chi	Quando
UE SEGRETISSIMO: Classificazione riservata esclusivamente a informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare danni di eccezionale gravità agli interessi fondamentali dell'Unione europea o di uno o più Stati membri [16.1]	La manomissione di informazioni classificate come UE SEGRETISSIMO potrebbe: — Minacciare direttamente la stabilità della UE o di uno dei suoi Stati membri o di paesi amici — Danneggiare in modo estremamente grave le relazioni con i governi amici — Causare direttamente una grossa perdita di vite umane — Arrecare danni di eccezionale gravità all'efficacia operativa o alla sicurezza degli Stati membri o alle forze di altri partner o compromettere l'efficacia di operazioni di sicurezza o di intelligence di estrema importanza — Danneggiare gravemente e per lungo tempo l'economia della UE o degli Stati membri	Persone debitamente autorizzate (originatori), direttori generali, capi servizio [17.1] L'originatore indica la data, un termine o un evento a partire dal quale le informazioni in esso contenute potranno essere declassate o declassificate. [16.2] In caso contrario, esso verifica almeno ogni cinque anni che la classificazione iniziale del documento sia tuttora necessaria [17.3]	La classificazione UE SEGRETISSIMO deve essere apposta su tutti i documenti aventi tali caratteristiche e, se del caso, deve essere affisso, a mano o a macchina, un contrassegno di sicurezza e/o di difesa — ESDP [16.4, 16.5, 16.3] Le classificazioni e i contrassegni di sicurezza UE sono apposti sulla parte superiore e inferiore di ogni pagina, al centro. Ogni pagina è numerata. Ciascun documento reca un numero di riferimento e una data, il numero di riferimento figura su ciascuna pagina Qualora i documenti siano distribuiti in più esemplari ognuno di essi reca un numero di copia che figura sulla prima pagina, a fianco del numero totale di pagine. Tutti gli allegati e il materiale accluso sono elencati sulla prima pagina [21.1]	Il declassamento o la declassificazione spetta unicamente all'originatore che comunica il cambiamento a tutti i destinatari successivi ai quali ha trasmesso l'originale o una copia del documento [17.3] I documenti UE SEGRETISSIMO sono distrutti dall'ufficio centrale di registrazione che ne è responsabile (o da una sottosezione dello stesso). Ogni documento distrutto viene elencato in un certificato di distruzione, firmato dal funzionario di controllo UE SEGRETISSIMO e dal funzionario che assiste alla distruzione il quale deve avere il nulla osta di sicurezza di grado UE SEGRETISSIMO. A tal fine nel repertorio viene inserita una nota. L'ufficio di registrazione tiene i certificati di distruzione, unitamente alle schede di distribuzione, per un periodo di dieci anni [22.5]	Le copie in ecceso e i documenti che non servono più devono essere distrutti [22.5] I documenti UE SEGRETISSIMO inclusi quelli classificati e poi scartati nella fase di preparazione di documenti UE SEGRETISSIMO, quali copie rovinate, bozze di lavoro, note dattiloscritte e copie su carta carbone devono essere distrutti sotto la sorveglianza di un funzionario UE SEGRETISSIMO mediante incenerimento o devono essere ridotti in pasta, sminuzzati o altrimenti ridotti in una forma irriconoscibile e non ricostituibile [22.5]

Classificazione	Quando	Chi	Apposizione delle classificazioni	Declassamento/declassificazione/distruzione	
				Chi	Quando
UE SEGRETO: Classificazione riservata esclusivamente a informazioni e a materiali la cui divulgazione non autorizzata potrebbe ledere gravemente gli interessi fondamentali dell'Unione europea o di uno o più Stati membri [16.1]	La manomissione di informazioni classificate come UE SEGRETO potrebbe: — Provocare tensioni a livello internazionale — Recare grave pregiudizio alle relazioni con governi amici — Comportare la minaccia della perdita di vite umane o compromettere seriamente l'ordine pubblico, la sicurezza individuale o la libertà Arrecare gravi danni all'efficacia operativa o alla sicurezza delle forze degli Stati membri o di altri contributori ovvero all'ininterrotta efficacia di operazioni di sicurezza o intelligence di grande importanza — Arrecare danni ingenti agli interessi finanziari, monetari, economici e commerciali della UE o di uno dei suoi Stati membri	Persone autorizzate (originatori), direttori generali, capi servizio [17.1] L'originatore indica la data o un termine a partire dal quale le informazioni in esso contenute potranno essere declassate o declassificate. [16.2] In caso contrario, esso verifica almeno ogni cinque anni che la classificazione iniziale del documento sia tuttora necessaria [17.3]	La classificazione UE SEGRETO deve essere apposta su tutti i documenti aventi tali caratteristiche e, se del caso, deve essere affisso, a mano o a macchina, un contrassegno di sicurezza e/o di difesa — ESDP [16.4, 16.5, 16.3] Le classificazioni e i contrassegni di sicurezza UE sono apposti sulla parte superiore e inferiore di ogni pagina, al centro. Ogni pagina è numerata. Ciascun documento reca un numero di riferimento e una data. Il numero di riferimento figura su ciascuna pagina Qualora i documenti siano distribuiti in più esemplari ognuno di essi reca un numero di copia che figura sulla prima pagina, a fianco del numero totale di pagine. Tutti gli allegati e il materiale accluso sono elencati sulla prima pagina [21.1]	Il declassamento o la declassificazione spetta unicamente all'originatore che comunica il cambiamento a tutti i destinatari successivi ai quali ha trasmesso l'originale o una copia del documento [17.3] I documenti UE SEGRETO sono distrutti dall'ufficio di registrazione che ne è responsabile, sotto la sorveglianza di una persona con nulla osta di sicurezza. I documenti UE SEGRETO distrutti sono elencati in un certificato di distruzione firmato, detenuto dall'ufficio di registrazione, unitamente alle schede di distruzione, per almeno tre anni [22.5]	Le copie in eccesso e i documenti che non servono più devono essere distrutti [22.5] I documenti UE SEGRETO inclusi quelli classificati e poi scartati nella fase di preparazione di documenti UE SEGRETO, quali copie rovinate, bozze di lavoro, note dattiloscritte e copie su carta carbone devono essere distrutti mediante incenerimento o devono essere ridotti in pasta, sminuzzati o altrimenti ridotti in una forma irriconoscibile e non ricostituibile [22.5]

Classificazione	Quando	Chi	Apposizione delle classificazioni	Declassamento/declassificazione/distruzione	
				Chi	Quando
UE RISERVATISSIMO classificazione riservata a informazioni e materiali la cui divulgazione non autorizzata lederebbe gli interessi fondamentali dell'Unione europea o di uno o più Stati membri [16.1]	La manomissione di informazioni classificate come UE RISERVATISSIMO potrebbe: — Recare un concreto pregiudizio alle relazioni diplomatiche, provocando proteste formali o altre sanzioni — Mettere a repentaglio la sicurezza o la libertà individuali — Arrecare danni all'efficacia operativa o alla sicurezza delle forze degli Stati membri o di altri contributori ovvero all'efficacia di importanti operazioni di sicurezza o intelligence — Compromettere in modo sostanziale l'efficienza finanziaria delle grandi organizzazioni — Ostacolare le indagini o agevolare le forme gravi di criminalità Ripercuotersi in modo sostanziale contro gli interessi finanziari, monetari, economici e commerciali della UE o dei suoi Stati membri — Ostacolare seriamente l'elaborazione o la realizzazione delle principali politiche comunitarie — Bloccare o perturbare seriamente importanti attività della UE	Persone autorizzate (originatori), direttori generali, capi servizio [17.1] L'originatore indica la data o un termine a partire dal quale le informazioni in esso contenute potranno essere declassate o declassificate. In caso contrario, esso verifica almeno ogni cinque anni che la classificazione iniziale del documento sia ancora necessaria [17.3]	La classificazione UE RISERVATISSIMO deve essere apposta su tutti i documenti aventi tali caratteristiche e, se del caso, deve essere affisso, a mano, a macchina, o a stampa su carta prestampigliata, registrata un contrassegno di sicurezza e/o di difesa — ESDP [16.4, 16.5, 16.3] Le classificazioni UE sono apposte sulla parte superiore e inferiore di ogni pagina, al centro. Ogni pagina è numerata. Ciascun documento reca un numero di riferimento e una data. Tutti gli allegati e il materiale accluso sono elencati sulla prima pagina [21.1]	Il declassamento o la declassificazione spetta unicamente all'originatore che comunica il cambiamento a tutti i destinatari succesivi ai quali ha trasmesso l'originale o una copia del documento [17.3] I documenti UE RISERVATISSIMO sono distrutti dall'ufficio di registrazione che ne è responsabile, sotto la sorveglianza di una persona abilitata. La loro distruzione è registrata conformemente alle norme nazionali e, per la Commissione e gli organismi decentrati della UE, in base alle istruzioni del presidente [22.5]	Le copie in eccesso e i documenti che non servono più devono essere distrutti [22.5] I documenti UE RISERVATISSIMO inclusi quelli classificati e poi scartati nella fase di preparazione di documenti UE RISERVATISSIMO, quali copie rovinate, bozze di lavoro, note dattiloscritte e copie su carta carbone devono essere distrutti mediante incenerimento o devono essere ridotti in pasta, sminuzzati o altrimenti ridotti in una forma irriconoscibile e non ricostituibile [22.5]

Classificazione	Quando	Chi	Apposizione delle classificazioni	Declassamento/declassificazione/distruzione	
				Chi	Quando
UE RISERVATO: Classificazione riservata a informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare danno agli interessi dell'Unione europea o di uno o più Stati membri [16.1]	La manomissione di informazioni classificate come UE RISERVATO potrebbe: — Avere ripercussioni negative sulle relazioni diplomatiche — Provocare notevoli difficoltà a singole persone — Rendere più difficile il mantenimento dell'efficacia operativa o della sicurezza delle forze degli Stati membri o altri contributori — Provocare perdite finanziarie o più facili profitti o vantaggi indebiti per singoli individui o società — Determinare il mancato rispetto dell'impegno di mantenere la riservatezza di informazioni fornite da terzi Provocare il mancato rispetto degli obblighi normativi in materia di divulgazione di informazioni — Mettere a repentaglio le indagini o agevolare la criminalità — Svantaggiare la UE o i suoi Stati membri nei negoziati di carattere commerciale o politico con terzi — Ostacolare un'efficace elaborazione o realizzazione delle politiche dell'UE — Compromettere il corretto funzionamento della UE e delle sue attività	Persone autorizzate (originatori), direttori generali, capi servizio [17.1] L'originatore indica la data, un termine o un evento a partire dal quale le informazioni in esso contenute potranno essere declassate o declassificate [16.2]. In caso contrario, esso verifica almeno ogni cinque anni che la classificazione iniziale del documento sia ancora necessaria [17.3]	La classificazione UE RISERVATO deve essere apposta su tutti i documenti aventi tali caratteristiche e, se del caso, deve essere affisso, in modo meccanico o elettronico, un contrassegno di sicurezza e/o di difesa — ESDP [16.4, 16.5 e 16.3] Le classificazioni e i contrassegni di sicurezza UE sono apposti sulla parte superiore di ogni pagina. Tutte la pagine devono essere numerate. Ciascun documento reca un numero di riferimento e una data [21.1]	La declassificazione spetta unicamente all'originatore che comunica il cambiamento a tutti i destinatari successivi ai quali ha trasmesso l'originale o una copia del documento [17.3] I documenti UE RISERVATO sono distrutti dall'ufficio di registrazione che ne è responsabile o dall'utente, conformemente alle istruzioni del presidente [22.5]	Le copie in eccesso e i documenti che non servono più devono essere distrutti [22.5]

Appendice 3

Linee direttrici per la comunicazione di informazioni classificate UE a Stati terzi o organizzazioni internazionali: livello 1 cooperazione

PROCEDURE

1. La facoltà di decidere la trasmissione di informazioni classificate UE a paesi che non sono membri sull'Unione europea o ad altre organizzazioni internazionali la cui politica in materia di sicurezza e la relativa normativa sono paragonabili a quelle dell'UE spetta alla Commissione in quanto Collegio.

2. In attesa che venga concluso un accordo sulla sicurezza, il membro della Commissione responsabile per le questioni della sicurezza è competente per l'esame delle richieste di trasmissione di informazioni classificate UE.

3. Il membro della Commissione a ciò preposto deve:
   — chiedere il parere degli originatori delle informazioni classificate UE da trasmettere,
   — stabilire i necessari contatti con gli organismi preposti alla sicurezza degli Stati o organizzazioni internazionali che ne sono i destinatari, per verificare l'idoneità della loro politica e normativa in materia di sicurezza a garantire che le informazioni classificate comunicate siano protette conformemente alle presenti norme di sicurezza,
   — chiedere il parere del gruppo consultivo della Commissione per le politiche della sicurezza quanto alla fiducia che può essere riposta negli Stati o organismi internazionali che ne sono destinatari.

4. Il membro della Commissione responsabile per le questioni della sicurezza deve inoltrare alla Commissione la richiesta e il parere formulato dal gruppo consultivo della Commissione per le politiche della sicurezza.

NORME DI SICUREZZA CHE DEVONO ESSERE APPLICATE DAI DESTINATARI

5. Il membro della Commissione responsabile per le questioni della sicurezza notifica agli Stati o alle organizzazioni internazionali destinatari la decisione della Commissione di autorizzare la comunicazione di informazioni classificate UE.

6. La decisione prende effetto soltanto previa garanzia scritta da parte dei destinatari che:
   — l'informazione sarà utilizzata ai soli scopi concordati,
   — sarà protetta conformemente alle presenti norme di sicurezza e in particolare alle disposizioni speciali riportate qui di seguito.

7. Personale

   a) Il numero di funzionari aventi accesso alle informazioni classificate UE è rigorosamente limitato, secondo il principio della necessità di sapere, alle persone le cui funzioni lo richiedano.

   b) Tutti i funzionari o cittadini autorizzati ad accedere alle informazioni classificate UE RISERVATISSIMO o di grado superiore sono in possesso di un attestato per un determinato grado di protezione o dell'equivalente nulla osta di sicurezza l'uno e l'altro emessi dal proprio governo nazionale.

8. Trasmissione di documenti

   a) Le procedure pratiche per la trasmissione di documenti sono decise mediante accordo. In attesa della conclusione di tale accordo si applicano le disposizioni della sezione 21. L'accordo dovrà fornire in particolare indicazioni precise sulle sezioni dell'Ufficio di registrazione a cui devono essere inoltrate le informazioni classificate UE.

   b) Se l'autorizzazione della Commissione riguarda la comunicazione di informazioni classificate anche di grado UE SEGRETISSIMO, lo Stato o l'organizzazione internazionale che ne sono destinatari istituiscono un ufficio centrale di registrazione UE, eventualmente suddiviso in sottosezioni. Tali sottosezioni devono applicare disposizioni rigorosamente equivalenti a quelle della sezione 22 delle presenti disposizioni in materia di sicurezza.

9. Registrazione

   Non appena riceve un documento classificato UE RISERVATISSIMO o di grado superiore, l'ufficio di registrazione lo annota in un registro speciale dell'organizzazione, suddiviso in colonne per la data di ricezione, dettagli del documento (data, numero di riferimento e di copia), la classificazione, il titolo, il nome o la qualifica del ricevente, la data di ritorno della ricevuta e la data di rinvio del documento all'originatore UE o dell'avvenuta distruzione.

10. Distruzione

a) I documenti classificati UE vengono distrutti secondo le istruzioni riportate nella sezione 22 delle presenti disposizioni in materia di sicurezza. L'avvenuta distruzione di documenti classificati UE SEGRETO e UE SEGRETISSIMO è attestata con certificati inviati in copia all'ufficio di registrazione UE che li aveva trasmessi.

b) I documenti classificati UE sono inclusi nei programmi di distruzione d'emergenza predisposti per i documenti classificati degli organismi destinatari.

11. Protezione dei documenti

Non sarà tralasciata alcuna misura che possa impedire l'accesso di persone non autorizzate alle informazioni classificate UE.

12. Copie, traduzioni ed estratti

È vietato fotocopiare o tradurre un documento classificato UE RISERVATISSIMO o UE SEGRETO, oppure estrarne brani senza l'autorizzazione del responsabile della sicurezza, che registrerà e controllerà copie, traduzioni o estratti apponendovi, se necessario, una stampigliatura.

La riproduzione o traduzione di un documento classificato UE SEGRETISSIMO può essere autorizzata soltanto dall'autorità d'origine, che preciserà il numero di copie autorizzate: se non è possibile risalire a tale autorità, la richiesta è deferita al servizio di sicurezza della Commissione.

13. Violazioni della sicurezza

In caso di violazione, presunta o reale, delle norme di sicurezza per un documento classificato UE, si dovrebbe immediatamente procedere, fatta salva la conclusione di un accordo in materia di sicurezza, a:

a) effettuare un'indagine per accertare le circostanze di detta violazione;

b) informare il servizio di sicurezza della Commissione, l'autorità nazionale competente in materia di sicurezza e l'autorità d'origine o dichiarare esplicitamente, se del caso, che quest'ultima non è stata informata;

c) adottare misure concrete per limitare al minimo gli effetti della violazione;

d) riesaminare e applicare le misure atte ad impedire nuovi episodi di questo tipo;

e) porre in atto tutte le misure raccomandate dal servizio di sicurezza della Commissione per impedire il verificarsi di nuovi episodi.

14. Ispezioni

Il servizio di sicurezza della Commissione sarà autorizzato, con il consenso degli Stati o delle organizzazioni internazionali interessati, ad effettuare una valutazione dell'efficacia delle misure prese a protezione delle informazioni classificate UE che sono state comunicate a terzi.

15. Relazioni

Fatta salva la conclusione di accordi in materia di sicurezza, gli Stati o le organizzazioni internazionali dovrebbero, fintanto che detengono informazioni classificate UE, presentare una relazione annuale a conferma del rispetto delle presenti disposizioni in materia di sicurezza, entro una data specificata al momento in cui è stata autorizzata la comunicazione dell'informazione.

Appendice 4

Linee direttrici per la comunicazione di informazioni classificate UE a Stati terzi o organizzazioni internazionali: livello 2 cooperazione

PROCEDURE

1. La facoltà di comunicare informazioni classificate UE a Stati terzi o organizzazioni internazionali la cui politica e normativa di sicurezza sono molto diverse da quelle dell'UE spetta all'originatore. La facoltà di decidere la trasmissione di informazioni classificate UE all'interno della Commissione spetta alla Commissione in quanto Collegio.

2. In linea di principio, è limitata alle informazioni classificate fino al grado UE SEGRETO compreso: ne sono escluse le informazioni classificate protette da speciali contrassegni di sicurezza.

3. In attesa che venga concluso un accordo sulla sicurezza, il membro della Commissione responsabile per le questioni della sicurezza è competente per l'esame delle richieste di trasmissione di informazioni classificate UE.

4. Il membro della Commissione a ciò preposto deve:
   — chiedere il parere degli originatori delle informazioni classificate UE da trasmettere,
   — stabilire i necessari contatti con gli organismi preposti alla sicurezza degli Stati o organizzazioni internazionali destinatari per avere informazioni sulla loro politica e la loro normativa in materia di sicurezza e in particolare per compilare una tabella in cui sono messe a confronto le classificazioni applicate nell'UE e quelle dello Stato o dell'organizzazione interessata,
   — organizzare una riunione del gruppo consultivo della Commissione per le politiche della sicurezza o, se necessario con la procedura di approvazione tacita, indagare presso le autorità nazionali competenti in materia di sicurezza per ottenere il parere gruppo consultivo della Commissione per le politiche della sicurezza.

5. Il parere del gruppo consultivo della Commissione per le politiche della sicurezza deve riguardare:
   — la fiducia che si può riporre negli Stati o organizzazioni internazionali destinatari allo scopo di valutare i rischi di sicurezza che corrono l'UE o gli Stati membri,
   — la valutazione della capacità dei destinatari di proteggere le informazioni classificate e comunicate dall'UE.
   — le proposte circa le procedure pratiche per il trattamento delle informazioni classificate UE (fornendo versioni parziali di un testo, per esempio) e dei documenti trasmessi (mantenendo o cancellando le diciture di classificazione UE, contrassegni specifici ecc.),
   — il declassamento o la declassificazione prima che le informazioni siano comunicate agli Stati o organizzazioni internazionali destinatari.

6. Il membro della Commissione responsabile per le questioni della sicurezza deve inoltrare alla Commissione la richiesta e il parere formulato dal gruppo consultivo della Commissione per le politiche della sicurezza.

NORME DI SICUREZZA CHE DEVONO ESSERE APPLICATE DAI DESTINATARI

7. Il membro della Commissione responsabile per le questioni della sicurezza notifica agli Stati o alle organizzazioni internazionali destinatari la decisione della Commissione di autorizzare la comunicazione di informazioni classificate UE e le restrizioni relative a quest'ultime.

8. La decisione prende effetto soltanto previa garanzia scritta da parte dei destinatari che:
   — l'informazione sarà utilizzata ai soli scopi concordati,
   — sarà protetta conformemente alle disposizioni della Commissione.

9. Si applicano le norme di protezione di seguito esposte a meno che la Commissione, sentito il parere tecnico del Gruppo consultivo della Commissione per le politiche della sicurezza, decida di adottare una particolare procedura per il trattamento dei documenti classificati UE (cancellando la menzione della classificazione UE, contrassegni specifici ecc.).

10. Personale

   a) Il numero dei funzionari aventi accesso alle informazioni classificate UE è rigorosamente ristretto, secondo il principio della necessità di sapere, alle persone le cui funzioni lo richiedono.

   b) Tutti i funzionari o i cittadini autorizzati ad accedere alle informazioni classificate comunicate dalla Commissione devono avere un nulla osta di sicurezza o un'autorizzazione nazionale per accedere a un determinato livello equivalente a quello dell'UE, secondo la definizione di cui alla tabella comparativa.

   c) I nulla osta di sicurezza o autorizzazioni nazionali sono inviati per informazione al presidente.

11. Trasmissione di documenti

Le procedure pratiche per la trasmissione di documenti sono decise mediante accordo. In attesa della conclusione di tale accordo si applicano le disposizioni della sezione 21. L'accordo dovrà specificare in particolare gli uffici di registrazione ai quali devono essere inoltrate le informazioni classificate UE e gli indirizzi esatti ai quali devono essere inoltrati i documenti nonché il corriere o i servizi postali usati per la trasmissione delle informazioni classificate UE.

12. Registrazione al momento dell'arrivo

La NSA dello Stato destinatario o il suo equivalente, che riceve le informazioni classificate inviate dalla Commissione a nome del proprio governo, ovvero l'ufficio di sicurezza dell'organizzazione internazionale destinataria, istituisce uno speciale registro per annotare le informazioni classificate UE all'atto del ricevimento. Il registro contiene colonne con l'indicazione della data, dettagli del documento (data, sigla e numero di esemplari), classificazione, titolo, nome o titolo del destinatario, data del ritorno della ricevuta e la data del rinvio del documento all'UE o quella della distruzione del documento.

13. Rinvio dei documenti

Il destinatario che rinvia un documento classificato alla Commissione, procede come indicato al precedente paragrafo «Trasmissione di documenti».

14. Protezione

a) I documenti che non sono in uso, sono custoditi in un contenitore di sicurezza omologato per la custodia di materiali dello stesso grado di classificazione, classificati a livello nazionale. Il contenitore non reca indicazioni del contenuto che è accessibile soltanto a persone autorizzate a trattare informazioni classificate UE. Per quanto riguarda le serrature a combinazione, questa è nota soltanto ai funzionari dello Stato o dell'organizzazione che sono autorizzati ad accedere alle informazioni classificate UE custodite nel contenitore ed è sostituita ogni sei mesi o quando un funzionario viene trasferito, oppure se a uno dei funzionari che conoscono la combinazione viene ritirato il nulla osta di sicurezza o se vi è un rischio di violazione.

b) I documenti classificati UE sono tolti dal contenitore di sicurezza solo dai funzionari che hanno ricevuto il nulla osta per l'accesso ai documenti classificati UE e hanno necessità di sapere. Essi sono responsabili della custodia sicura dei documenti finché ne sono in possesso e in particolare garantiscono che nessuna persona non autorizzata abbia accesso ai documenti. Assicurano anche che i documenti siano custoditi in un contenitore di sicurezza quando hanno finito di consultarli e al di fuori dell'orario di lavoro.

c) Non è permesso fare fotocopie di un documento classificato UE RISERVATISSIMO o di grado superiore né trarne estratti senza l'autorizzazione del Servizio di sicurezza della Commissione.

d) È necessario che la procedura per una rapida e totale distruzione dei documenti in caso di emergenza sia definita e confermata in collaborazione con il servizio di sicurezza della Commissione.

15. Sicurezza materiale

a) Quando non sono usati, i contenitori di sicurezza adibiti alla custodia dei documenti classificati UE devono essere chiusi a chiave in permanenza.

b) Il personale addetto alla manutenzione o alle pulizie che deve entrare o lavorare in una stanza in cui sono situati i contenitori di sicurezza deve essere scortato continuamente da un membro del servizio di sicurezza dello Stato o dell'organizzazione o dal funzionario che è direttamente responsabile per la supervisione della sicurezza della stanza stessa.

c) Al di fuori dell'orario di lavoro normale (la notte, nei fine settimana e nei giorni festivi) i contenitori di sicurezza che custodiscono documenti classificati UE sono protetti da una guardia o da un sistema d'allarme automatico.

16. Violazioni della sicurezza

Se si è verificata o si sospetta che si sia verificata una violazione della sicurezza relativamente a un documento classificato UE occorre immediatamente provvedere a:

a) inviare subito una relazione al servizio di sicurezza della Commissione o alla NSA dello Stato membro che ha preso l'iniziativa di inviare documenti (con copia al servizio di sicurezza della Commissione);

b) condurre un'inchiesta al termine della quale è presentata al servizio di sicurezza una relazione completa [cfr. a) supra]. Sono poi adottate le misure necessarie per porre rimedio alla situazione.

17. Ispezioni

    Il servizio di sicurezza della Commissione sarà autorizzato, con il consenso degli Stati o delle organizzazioni internazionali interessati, ad effettuare una valutazione dell'efficacia delle misure prese a protezione delle informazioni classificate UE che sono state comunicate a terzi.

18. Relazioni

    Fatta salva la conclusione di accordi in materia di sicurezza, gli Stati o le organizzazioni internazionali dovrebbero, fintanto che detengono informazioni classificate UE, presentare una relazione annuale a conferma del rispetto delle presenti disposizioni in materia di sicurezza, entro una data specificata al momento in cui è stata autorizzata la comunicazione dell'informazione.

Appendice 5

Linee direttrici per la comunicazione di informazioni classificate UE a Stati terzi o organizzazioni internazionali: livello 3 cooperazione

PROCEDURE

1. Occasionalmente, in circostanze particolari, è possibile che la Commissione intenda cooperare con Stati o organizzazioni che non possono dare le garanzie richieste dalle presenti disposizioni in materia di sicurezza ma che tale cooperazione richieda la comunicazione di informazioni classificate UE.

2. La facoltà di comunicare informazioni classificate UE a Stati terzi o organizzazioni internazionali la cui politica e normativa di sicurezza sono molto diverse da quelle dell'UE spetta all'originatore. La facoltà di decidere la trasmissione di informazioni classificate UE all'interno della Commissione spetta alla Commissione in quanto Collegio.

   In linea di principio, è limitata alle informazioni classificate fino al grado UE SEGRETO compreso: ne sono escluse le informazioni classificate protette da speciali contrassegni di sicurezza.

3. La Commissione valuta se comunicare le informazioni classificate, considera la necessità di sapere dei destinatari e decide quali informazioni classificate possano essere comunicate.

4. Se la Commissione è favorevole, il membro della Commissione responsabile per le questioni della sicurezza:
   — chiedere il parere degli originatori delle informazioni classificate UE da trasmettere,
   — organizzare una riunione del gruppo consultivo della Commissione per le politiche della sicurezza o, se necessario con la procedura di approvazione tacita, indagare presso le autorità nazionali competenti in materia di sicurezza per ottenere il parere gruppo consultivo della Commissione per le politiche della sicurezza.

5. Il parere del gruppo consultivo della Commissione per le politiche della sicurezza deve riguardare:

   a) una valutazione dei rischi di sicurezza corsi dall'UE o dagli Stati membri;

   b) il grado di classificazione delle informazioni che possono essere comunicate;

   c) il declassamento o la declassificazione prima di comunicare le informazioni;

   d) le procedure per il trattamento dei documenti da divulgare (vedi il paragrafo successivo);

   e) sui metodi di trasmissione (servizi postali, sistemi di telecomunicazioni pubblici o protetti, valigia diplomatica, corrieri autorizzati, ecc.).

6. I documenti comunicati a Stati o organizzazioni che rientrano in questa appendice sono predisposti, in linea di massima, senza un riferimento alla fonte o a una classificazione UE. Il gruppo consultivo della Commissione per le politiche della sicurezza può raccomandare:
   — l'uso di un contrassegno o codice specifico,
   — l'uso di un sistema di classificazione specifico che rapporta la sensibilità delle informazioni alle necessarie misure di controllo dei metodi usati dal destinatario per trasmettere i documenti.

7. Il presidente inoltra alla Commissione, affinché quest'ultima prenda una decisione, il parere formulato dal gruppo consultivo della Commissione per le politiche della sicurezza.

8. Dopo che la Commissione ha approvato la comunicazione di informazioni classificate UE e le procedure pratiche di attuazione, il servizio di sicurezza della Commissione stabilisce i necessari contatti con l'organismo preposto alla sicurezza dello Stato o organizzazione interessati per facilitare l'applicazione delle misure di sicurezza prospettate.

9. Il membro della Commissione responsabile per le questioni della sicurezza informa gli Stati membri sulla natura e la classificazione delle informazioni, elencando le organizzazioni e gli Stati ai quali queste possono essere comunicate, secondo quanto deciso dalla Commissione.

10. Il servizio di sicurezza della Commissione prende le misure necessarie per facilitare la valutazione di qualsiasi possibile danno e la revisione delle procedure.

    In caso di mutamento delle condizioni di cooperazione, la Commissione deve procedere a un riesame della materia.

NORME DI SICUREZZA CHE DEVONO ESSERE APPLICATE DAI DESTINATARI

11. Il membro della Commissione responsabile per le questioni della sicurezza notifica agli Stati o alle organizzazioni internazionali destinatari la decisione della Commissione di autorizzare la comunicazione di informazioni classificate UE, unitamente alle norme di protezione dettagliate proposte dal gruppo consultivo della Commissione per le politiche della sicurezza e approvata dalla Commissione stessa.

12. La decisione entra in vigore soltanto quando i destinatari danno assicurazione scritta:

— di non destinare le informazioni a un uso diverso dalla cooperazione decisa dalla Commissione,

— di dare alle informazioni la protezione richiesta dalla Commissione.

13. Trasmissione di documenti

a) Le procedure pratiche per la trasmissione di documenti sono concordate tra il servizio sicurezza della Commissione e gli organi preposti alla sicurezza degli Stati e organizzazioni internazionali destinatari. In particolare devono essere specificati gli indirizzi esatti per l'invio dei documenti.

b) I documenti classificati UE RISERVATISSIMO e gradi superiori sono trasmessi in doppia busta. La busta interna reca lo specifico timbro o codice convenuto e la menzione della classificazione particolare che è stata approvata per il documento. A ciascun documento classificato è acclusa una ricevuta. La ricevuta, di per sé non classificata, cita soltanto i dettagli del documento (sigla, data, numero di esemplari) e la lingua, ma non il titolo.

c) La busta interna è posta in un'altra busta che reca il numero del plico per consentire il rilascio di una ricevuta. La busta esterna non reca alcuna classificazione di sicurezza.

d) Ai corrieri è sempre fornita una ricevuta con il numero del plico.

14. Registrazione al momento dell'arrivo

La NSA dello Stato destinatario o il suo equivalente, che riceve le informazioni classificate inviate dalla Commissione per conto del suo governo, ovvero l'ufficio di sicurezza dell'organizzazione internazionale destinataria, istituisce uno speciale registro per annotare le informazioni classificate UE all'atto del ricevimento. Il registro è suddiviso in colonne che riportano l'indicazione della data, i dettagli del documento (data, sigla e numero di esemplari), la classificazione, il titolo, il nome o titolo del destinatario, la data del ritorno della ricevuta e la data del rinvio del documento all'UE o quella della distruzione del documento.

15. Utilizzazione e protezione delle informazioni classificate scambiate

a) Le informazioni a livello UE SEGRETO sono trattate da funzionari specificamente designati che sono autorizzati ad avere accesso alle informazioni aventi tale classificazione. Sono custodite in armadi di sicurezza di buona qualità che possono essere aperti soltanto da persone autorizzate ad avere accesso alle informazioni che contengono. I luoghi in cui detti armadi sono situati sono sorvegliati costantemente: un sistema di verifica garantisce che possono entrarvi soltanto le persone debitamente autorizzate. Le informazioni di livello UE SEGRETO sono inviate per valigia diplomatica, servizi postali e servizi di telecomunicazioni protetti. Un documento UE SEGRETO può essere copiato soltanto con l'accordo scritto dell'autorità d'origine. Tutte le copie sono registrate e controllate. Per tutte le operazioni relative a documenti UE SEGRETO sono rilasciate ricevute.

b) Le informazioni di livello UE RISERVATISSIMO sono trattate da funzionari debitamente designati e autorizzati a conoscere l'argomento. I documenti sono custoditi in armadi di sicurezza chiusi a chiave in luoghi controllati.

Le informazioni di livello UE RISERVATISSIMO sono inviate per valigia diplomatica, servizi postali militari e telecomunicazioni protette. L'organismo destinatario può farne copie, annotando il relativo numero e la distribuzione in appositi registri.

c) Le informazioni di livello UE RISERVATO sono trattate in luoghi non accessibili a personale non autorizzato e custodite in contenitori chiusi a chiave. I documenti possono essere inviati tramite i servizi postali pubblici come plico raccomandato in doppia busta; in casi di emergenza durante le operazioni, tramite sistemi di telecomunicazioni pubblici non protetti. I destinatari possono fotocopiarli.

d) Le informazioni non classificate non richiedono speciali misure di protezione e possono essere inviate per posta e tramite i sistemi pubblici di telecomunicazioni. I destinatari possono copiarle.

16. Distruzione

I documenti che non servono più devono essere distrutti. Nel caso di documenti UE RISERVATO E UE RISERVATISSIMO, viene inserita una nota nei registri speciali. Nel caso di documenti del livello UE SEGRETO, sono rilasciati certificati di distruzione firmati da due testimoni della distruzione.

17. Violazioni della sicurezza

Se informazioni di livello UE RISERVATISSIMO o UE SEGRETO sono compromesse o se vi è un sospetto in tal senso, la NSA dello Stato o il capo del servizio di sicurezza dell'organizzazione conduce un'inchiesta per appurare le circostanze della violazione e notifica i risultati dell'inchiesta al servizio di sicurezza della Commissione. Si adottano quindi i provvedimenti atti a migliorare le procedure o i metodi di custodia inadeguati che possano essere all'origine della violazione.

Appendice 6

ELENCO DELLE ABBREVIAZIONI

CCAC	Commissione consultiva per gli acquisti e i contratti
CrA	Autorità Crypto
CISO	Responsabile della sicurezza informatica a livello centrale
COMPUSEC	Sicurezza informatica
COMSEC	Sicurezza delle comunicazioni
CSO	Ufficio di sicurezza della Commissione
ESDP	Politica europea di sicurezza e di difesa
ICUE	Informazioni classificate UE
IA	Autorità INFOSEC
INFOSEC	Sicurezza dell'informazione
IO	Proprietario delle informazioni
ISO	Organizzazione internazionale di normalizzazione
TI	Tecnologie dell'informazione
LISO	Responsabile della sicurezza informatica a livello locale
LSO	Responsabile della sicurezza a livello locale
MSO	Responsabile della sicurezza della riunione
NSA	Autorità nazionali di sicurezza
PC	Personal Computer
RCO	Funzionario di controllo dell'ufficio di registrazione
SAA	Autorità di accreditamento in materia di sicurezza
SecOPS	Procedure operative di sicurezza
SSRS	Dichiarazione relativa ai requisiti di sicurezza specifici del sistema
TA	Autorità Tempest
TSO	Proprietario dei sistemi tecnici

03A08079

GIANFRANCO TATOZZI, *direttore* FRANCESCO NOCITA, *redattore*

(6501430/1) Roma, 2003 - Istituto Poligrafico e Zecca dello Stato S.p.A. - S.

€ 3,20